

Surveillance Camera (CCTV) Procedure

At a glance ...

- The use of surveillance cameras can be particularly privacy intrusive. Their use must be necessary, proportionate and adequate for their stated purpose.
- The Council will have regard to relevant Codes of Practice in its use of surveillance cameras.
- There must be a clear and lawful justification for the use of surveillance cameras. Other options for achieving the same ends must be considered.
- A surveillance camera system specific Data Protection Impact Assessment (DPIA) must be completed for all new systems before they become operational. DPIAs will also be completed for existing systems.
- There must be appropriate information and signage and privacy information to advise of the use of surveillance cameras, except for covert surveillance.
- The Council's [Regulation of Investigatory Powers Act and Surveillance Policy and guidance](#) applies to the use of covert surveillance (i.e. the use of CCTV to target surveillance of known individuals or groups).
- Images and recordings from surveillance camera systems will be held for no longer than 31 days, unless there is a documented rationale otherwise.
- Footage which is the subject of a request for disclosure must be securely held until all actions associated with the request are complete.
- Request for surveillance camera images by people asking for their own data (i.e. a Subject Access Request) or as part of Freedom of Information request will be referred to the Complaints and Information Team.
- All other requests to disclose surveillance camera images will be handled locally but in accordance with this Procedure and a local register will be kept of such disclosures.
- All suppliers of surveillance cameras systems will have a contract with the Council that has appropriate data protection clauses.
- All surveillance camera systems will have a designated responsible owner who may appoint system operators.
- Surveillance camera systems will be evaluated on an annual basis.
- A corporate register of all surveillance camera systems will be maintained by the Information Governance Team.
- The Council's Data Protection Officer (DPO) will be the Senior Responsible Officer for overt surveillance camera systems and will be the Council's point of contact with the Surveillance Camera Commissioner.

Background

1. The County Council operates surveillance cameras including Closed Circuit Television (CCTV) cameras for a number of purposes. This includes the security of Council premises and car parks; automatic number plate recognition outside schools; and for traffic enforcement, etc.
2. The use of surveillance cameras is regulated by law and there are a number of codes of practice that staff should be aware of that are relevant to their use:
3. The role of the Surveillance Camera Commissioner (SCC) is to encourage compliance with the [Surveillance Camera Code of Practice](#). The Protection of Freedoms Act 2012 requires all local authorities operating surveillance cameras to pay due regard to this Code of Practice.
4. The role of the Information Commissioner's Office (ICO) is to oversee implementation of data protection laws including the Data Protection Act 2018. The ICO [CCTV Code of Practice](#) provides guidance for use of surveillance systems and is designed to explain the legal requirements operators of surveillance cameras are required to meet to comply with data protection law.

Purpose

5. This procedure is to be followed when planning for or overtly using surveillance camera(s), including closed circuit television (CCTV), dashcams, body worn cameras, unmanned aerial systems (drones) etc.

Scope and Definitions

6. This procedure forms part of the suite of documents that comprise the Council's [Information Governance Framework](#) and is a requirement of the [Information Compliance Policy](#).
7. All staff who have roles related to this procedure must be aware of and abide by it (see section on roles and responsibilities).
8. This procedure applies all overt surveillance cameras operated by Nottinghamshire County Council, regardless of whether mobile or fixed or the means by which they are put in place (i.e on bodies; in cars or other vehicles; on / in buildings; on drones etc).
9. This procedure does not apply to covert surveillance (e.g. targeted surveillance of known individuals or groups). There are strict rules on covert surveillance. Please refer to the County Council's [Regulation of Investigatory Powers Act and Surveillance Policy and guidance](#) and seek advice from the Council's Legal Services if covert surveillance is being considered.

10. A surveillance camera system is defined as the cameras and all the related hardware and software for transmitting, processing and storing the data which is captured.
11. Information in this procedure is used as a collective term primarily to describe personal data collected through the use of surveillance camera systems.
12. A data controller is defined as an organisation that determines the how and why personal data is collected and used. The Council is a data controller.
13. A data processor acts under the instruction of a data controller and collects and uses personal data on the controller's behalf. Surveillance camera system suppliers are data processors.
14. A data subject is defined as an identified or identifiable individual to whom personal data relates.

Principles & Commitments

15. The Council recognises that the use of surveillance cameras can be intrusive and is committed to ensuring that the relevant Codes of Practice inform its use of surveillance cameras.
16. A central register of all surveillance camera systems will be maintained by the Information Governance Team. All Departments will need to ensure that they provide information necessary to ensure that the register is complete and up-to-date.
17. Privacy considerations in respect of the planning and use of surveillance cameras will be documented. All new surveillance camera systems will only be implemented when a surveillance camera specific Data Protection Impact Assessment (DPIA) has been completed and signed-off (see [Appendix A](#)).
18. The Council will aim for all surveillance camera systems to have a completed DPIA and a plan will be put in place to achieve this.
19. DPIAs maybe aggregated where there is a common purpose and use, for instance at multiple locations (e.g. all County Offices).
20. The Council's Data Protection Officer will be the Senior Responsible Officer to the Council's use of overt surveillance cameras.
21. All surveillance camera systems will have a system owner who may appoint a system operator to undertake the day-to-day operation of the system.
22. Third party providers of surveillance camera systems to the Council will be a data processor for the Council and there will be a contract in place which takes account of data protection obligations to the Council and the law.
23. The Council recognises that the use of personal information must be fair, and personal information must be retained and processed securely.

24. Data obtained from the surveillance camera system will only be stored for as long as necessary and in accordance with the County Council's retention schedules.

The Legislative Framework

25. The operation of surveillance camera systems must be undertaken with due regard to the following legislation:
- a. The Data Protection Act (DPA) 2018;
 - b. The EU General Data Protection Regulation (GDPR) and laws implementing or supplementing the GDPR;
 - c. The Human Rights Act 1998;
 - d. The Regulation of Investigatory Powers Act 2000;
 - e. The Freedom of Information Act (FoIA) 2000;
 - f. The Protection of Freedoms Act (PoFA) 2012.
26. Where the operation of surveillance cameras are likely to record the movements of individuals, the GDPR and Data Protection Act will apply to the recording, use, storage, destruction and sharing of personal information.
27. Public authorities carrying out public functions are required to observe the obligations imposed by the Human Rights Act 1998. Recording the movements of individuals is most likely to require consideration of the right to respect an individual's privacy, as provided for under Article 8 of that Act. In order to be compliant, the use of surveillance cameras must be justified, in accordance with law, necessary and proportionate and in the interests of one of the following legitimate objectives:
- a. public safety;
 - b. for the prevention of disorder or crime;
 - c. or the protection of health or morals; or
 - d. for the protection of the rights and freedoms of others.
28. Staff undertaking covert surveillance with or without surveillance camera devices must comply with the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Codes of Practice issued in support of that legislation.
29. Covert surveillance may occur where there is a planned operation to target surveillance of known individuals or groups. RIPA can apply to monitoring via the use of surveillance cameras or CCTV that is primarily operated for another purpose. However, this procedure does not apply to such activities. Please refer to the County Council's [Regulation of Investigatory Powers Act and Surveillance Policy and guidance](#) and seek advice from the Council's Legal Services.

Planning a new surveillance camera system

30. Where there are plans to introduce a new surveillance camera system, the [CCTV Data Protection Impact Assessment \(DPIA\)](#) must be completed and submitted to the Council's Information Governance Team (data.protection@nottscc.gov.uk).

31. The DPIA will be reviewed by the Data Protection Officer (DPO) before being signed-off by the relevant Information Asset Owner (IAO) (i.e. Service Director). In signing off the DPIA, the IAO will have regard to DPO advice. Where a DPIA is signed off against the advice of the DPO, the IAO's rationale will be documented and the DPO may seek the input of the Council's Senior Information Risk Owner (SIRO).
32. In the event that the DPIA is not signed off by the IAO, the surveillance camera system must not be implemented.

The purpose of the surveillance camera system

33. When planning the use of the surveillance camera system it is important to identify the purpose of the system. For instance, for the purpose of the prevention or detection of crime in an area where there has been a spate of thefts. This can help understand whether the proposals fit under the law and what mitigations may need to be taken to ensure the surveillance system can be operated lawfully.
34. The purpose of the surveillance camera system needs to be a legitimate one and necessary to meet an identified pressing need and specified purpose. Such needs may be:
 - a. For prevention or detection of crime or apprehension of offenders;
 - b. For the personal safety of employees, service users or the general public
 - c. For health and safety,
 - d. Traffic enforcement
 - e. Traffic management
35. Surveillance cameras should not be used where there is no legitimate justification for their use.
36. The surveillance cameras should be suitable for the purposes for which they are being used. If being used for prevention or detection of crime, the images need to be suitable for the purposes of identifying suspects and be of a sufficient standard to be capable of being used in evidence.
37. Where a surveillance camera system has the potential to be used for more than one purpose, each of those purposes needs to be considered in order to determine whether its use is justified. If a surveillance camera system is designed for one purposes only it should not be used for another purpose unless such use is justified and has been authorised in advance.

Considering necessity and proportionality

38. Consideration must be given as to whether surveillance cameras are a proportionate response to a legitimate concern that needs to be addressed. This requires an assessment of what the impact surveillance cameras may be on individuals and their privacy, and what can be done to mitigate this impact. The more the impact can be mitigated the more likely the use may be proportionate.

39. Cameras should not be located in places where individuals expect privacy, for instance, changing rooms. Such use is likely to be considered invasive and is unlikely to be capable of being justified as proportionate unless there are particularly serious problems that warrant such use, for instance, to prevent serious harm. Extra care would need to be taken to monitor use to ensure that the use of cameras is reviewed regularly to determine if it is still justified.
40. Use of video and audio recording is considered more invasive given that audio could pick up the contents of private conversations and is unlikely to be justified in most circumstances. **If audio recordings are not required for the purposes of the surveillance camera system they should not be used.**
41. The surveillance camera system being proposed should be designed in a manner that the intrusion into individuals' private lives is considered and measures to limit intrusion should be put in place where possible. For instance, cameras should be situated so as not to overlook private properties.
42. Use of facial recognition or other biometric technologies are unlikely to be justified unless there is a strong argument to justify their use.
43. It may be appropriate to undertake some form of consultation with those who will benefit from or be affected by the use of surveillance cameras to help assess whether there is a legitimate aim and a pressing need for surveillance cameras, and whether the system itself is a proportionate response.
44. If there are less intrusive means of dealing with the issues that the surveillance cameras are designed to address, these other measures should be considered first before deciding that surveillance cameras are appropriate. Evidence should be kept of the options considered and rationale for decision making.

Camera location, use of signage and information

45. Use of surveillance cameras must be transparent and sited at a location to capture clear good quality images but not in an area that would be overly intrusive. Staff and the public must be made aware of the operation of surveillance cameras. Therefore consideration needs to be given to the location of surveillance cameras and sufficient signage to alert staff and visitors to their use.
46. Signage will clearly indicate surveillance cameras are in operation and be prominently placed. The signage will also:
 - a. make it clear that Nottinghamshire County Council is responsible for operating the system,
 - b. the purpose/s of the surveillance system
 - c. provide a contact number for further information for those with queries about usage and who wish to access recordings. This can be the contact number of the Information Governance Team telephone number 0115 8043800 (on behalf of the DPO) or the system owner (see roles and responsibilities section)
47. Examples of appropriate and inappropriate signage is given at [Appendix B](#).

48. The Information Governance Team will produce a corporate surveillance camera / CCTV Privacy notice but individual service specific privacy notices should reference the use of surveillance camera system(s) where appropriate.

Guidance for the use of a surveillance camera system

Security and retention of recorded material

49. In order to ensure that information remains secure, only a named and limited number of staff should be authorised to access it. Access should be limited to those who require it for a specific business reason. All surveillance camera material should be protected by appropriate security measures to safeguard against unauthorised access and use.
50. Images and information obtained from the surveillance camera system should be stored no longer than that which is strictly required for the stated purpose of the system's use. **This may vary, but will ordinarily be no longer than 31 days.**
51. Where System Owners, in conjunction with the IAO, decide to have a retention period of longer than 31 days for the routine operation of a system, a documented rationale must be kept for this decision.
52. The Council's corporate retention schedule indicates that CCTV footage will be retained until overwritten unless used in legal case, in which case the CCTV footage will become part of the case file.
53. Information must be securely destroyed once its purpose has been discharged and at the end of its retention period unless there is a documented reason to retain it (e.g. to support legal proceedings).
54. Deleted information should not be capable of being recovered. ICT security should be consulted on the appropriate method of deletion, in line with the [Council's Data Destruction Standard](#).

Keep supporting information accurate and up to date

55. Where the surveillance camera system captures data that is cross referenced against other data (eg. number plate and car ownership details), and NCC is the data controller for that information, the databases relied upon should be kept accurate and up to date. If the database is provided by an external source, such as the DVLA, their responsibility to keep the database up to date should be included in the terms of our contract with them.

Evaluation

56. Surveillance camera systems must be evaluated on an annual basis to confirm ongoing compliance with the requirements of this procedure. Information Governance will liaise with system owners to complete an [evaluation form](#) when a review is due.

Operating Procedures

57. Clear rules and procedures should be put in place to help ensure that staff operating surveillance cameras are made aware of how to operate the surveillance cameras safely. Ideally this information should be provided on induction and training should also be provided to make staff aware of their obligations.
58. Localised procedures, complementing this corporate one, should set out which staff are responsible for the operation of the system and what their roles should be. See roles and responsibilities section below.
59. Staff operating surveillance camera systems shall be made aware of this procedure, any relevant operating procedures and have information governance training. Relevant staff will also undertake training in respect of local surveillance camera systems where it is made available.

Service providers operating surveillance cameras

60. Where a service provider is operating surveillance cameras for the County Council they are likely to be processing the County Council's personal data and the provider is classed as a data processor. The County Council can be held responsible for the actions of a data processor and be liable for breaches of the data protection or other privacy related legislation.
61. There must be a contract in place with any service providers operating surveillance cameras. The terms of the contract must specify any specific obligations that the service provider will comply with in order to help ensure that the service provider does not operate the surveillance camera system unlawfully.
62. The contract should ensure that the service provider is obliged to have regard to the Surveillance Camera Commissioner's Surveillance Camera Code of Practice and the Information Commissioner's CCTV Code of Practice when operating surveillance camera.
63. Transfer of data outside the [European Economic Area](#) is not allowed unless special legal safeguards are put in place and in some cases it may not be lawful to transfer personal data outside of the EEA. Advice from Legal Services should be obtained when appointing or reviewing contractual terms or prior to a service provider.

Complaints

64. The County Council's complaints procedure will apply to the handling of complaints related to surveillance camera operation. Complaints of this nature should be referred to the Complaints and Information team [email: complaints@nottscc.gov.uk / tel: 0115 977 2788] who will, where necessary, liaise with the DPO in relation to data protection issues that are raised. Departments operating surveillance cameras may be asked to provide information to the Complaints and Information Team.

65. Complaints may be handled as a data protection complaint if the complaint relates to the use of personal information. Such complaints should be notified as soon as possible to the Complaints and Information Team and within 24 hours at the latest.
66. Where complaints cannot be resolved through the internal complaints process they may be referred to the Information Commissioner's Office or the Local Government Ombudsman as appropriate.

Handling requests for information

67. The following paragraphs outline the types of requests that may be made for surveillance camera / CCTV images and how to deal with them. Because of the fairly short deletion timescales for images, a hold should be placed on the relevant material immediately upon receiving a request. Only when all actions associated with the request have been completed should images which are subject of the request be deleted.

Subject Access Requests

68. Under the Data Protection Act 2018, individuals have a right to know what personal information about them the Council holds and uses. They can exercise this right by making a Subject Access Request.
69. The Council has a [Subject Access Request Procedure](#) this details the process for SARs including timescales for response etc. The Council's Complaints and Information Team coordinates SARs for the Council including any CCTV data required as part of a SAR.
70. An individual whose image has been recorded by CCTV may have a right to view / receive a copy of images held by the Council, provided that:
 - a. The Council is supplied with sufficient information to be satisfied as to the identity of the person making the request
 - b. If an application is made by a legal representative, it must be confirmed that the individual is happy for the legal representative to make this request on their behalf.
 - c. The person making the request provides sufficient and accurate information about the time (within a + / - one hour accuracy), date and place to enable the Council to locate the information sought.
 - d. The person making the request is only shown / given access to information relevant to that particular search and which contains their own personal data only.
 - e. Data which discloses the identities of other individuals who may be identified from the same information will not be released unless those individuals have consented to the disclosure.
71. A form to be used when an individual is requesting surveillance camera images of themselves under a SAR is attached at [Appendix C](#).

72. A form to be used by young people housed in **Clayfields House Secure Children's Home** (or their representatives) requesting their information will be requested to is attached at [Appendix D](#).

73. Subject Access Requests may be refused by the Council:

- a. If the release of the information is likely to prejudice the prosecution of offenders
- b. Where a viewing / the provision of a copy is not actually possible.
- c. If the information provided is not detailed enough to allow data to be found, and the requester does not provide further detail on prompting.

74. Where a decision is taken not to disclose the requester will be notified in writing.

Third party requests to disclose surveillance camera (CCTV) footage

75. In limited circumstances, requests to view or receive copies of information generated by a surveillance camera (CCTV) systems may be made by third parties for any one or more of the following purposes or in other circumstances where an exemption applies under relevant legislation:

- a. The prevention or detection of crime
- b. The apprehension or prosecution of offenders
- c. The assessment or collection of tax or duty (or similar)
- d. Providing evidence in connection with legal proceedings (or prospective legal proceedings)
- e. Necessary to establish, exercise or defend legal rights.

76. The Data Protection Act 2018 allows for disclosures of this nature, particularly Schedule 2, 2(1) and Schedule 2, 5(3).

77. Third parties are required to show adequate grounds for disclosure of data within the above criteria and may be any of the following:

- a. Police authorities, (not just Nottinghamshire Constabulary).
- b. Statutory authorities with powers to prosecute, (e.g. Customs and Excise, Trading Standards etc.).
- c. Solicitors or insurance companies, on behalf of clients.
- d. Trade unions, on behalf of members.
- e. Claimants in civil proceedings.
- f. Accused persons or defendants in criminal proceedings.
- g. Other agencies, (as agreed by the Council and notified to the Information Commissioner) according to purpose and legal status.

78. Organisations applying to the Council for the disclosure of surveillance camera images under Schedule 2, 2(1) [in connection with the prevention or detection of crime or the apprehension or prosecution of offenders] are required to complete the relevant form at Appendix E or provide their own form with the equivalent information (Police Authorities sometimes have disclosure request forms). In

either case, the form should be signed by someone with sufficient seniority (e.g. Inspector or above within Police Authorities).

79. Organisations applying to the Council for the disclosure of surveillance camera images under Schedule 2, 5(3) [in connection with legal proceedings or to establish, exercise or defend legal rights] are required to complete the relevant form at Appendix F. Where a request is made by a representative of an individual, the representative must provide evidence that they are acting on the individual's behalf.
80. Information will only be disclosed if the Council judges that there are strong enough grounds to do so. If the Council decides to release the information, the following steps will be taken:
 - a. The requestor's identity will be verified.
 - b. The accuracy of the request will be verified (particularly that a valid lawful basis for the disclosure).
 - c. The requestor (or an authorised person acting on their behalf) will be shown / provided with a copy of the relevant footage only.
 - d. The viewing will take place in a private area, with adequate supervision. Camera footage should not be shown to a requestor in an open office or camera control room.
 - e. Only data which is specific to the request will be shown. It should not be possible to identify any other individual from the information being shown. Any footage showing other individuals will be blanked-out (either by means of electronic depixillation, or manual editing on the monitor screen) or otherwise redacted.
 - f. If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material will be sent to an authorised editing house for processing prior to being sent to the requester.
 - g. If the data is pending application for, or issue of, a court order or subpoena, but may be relevant to a request, the Council will ensure it is retained. A time limit will be imposed on such retention, which the requesting party will be notified of at the time of the request.
 - h. A log will be kept as evidence of all disclosed surveillance camera / CCTV images along with the relevant request forms.
81. Third party disclosure requests will be handled locally but the Complaints and Information Team will provide assistance responding to requests.
82. On rare occasions, a request may be made by a third party where a different Schedule 2 exemption from those listed above applies. On these occasions the Information Governance team will advise on the correct legal gateway and assess the grounds for disclosure.

Internal Requests for Information

83. In limited circumstances, requests to view or receive copies of information generated by a surveillance camera (CCTV) system may be made by NCC employees.
84. Disclosure is permitted where there is a clear purpose and justification for why footage is required. This purpose must be in line with the original purpose for which the surveillance camera system was installed.
85. A request for footage must be made to the relevant system owner. Requests must be made in writing.
86. Information will only be disclosed if the system owner judges that there are adequate grounds for disclosure. If they are in doubt, they should seek guidance from the Information Governance Team. If the information is released the following steps will be taken:
 - a. The requester will be shown / provided with a copy of the relevant footage only.
 - b. The viewing will take place in a private area, with adequate supervision. Camera footage must not be shown to a requestor in an open office or camera control room.
 - c. Only data which is specific to the request will be shown / provided.
87. The sharing request, decision made and justification should be documented using an Internal Personal Information Sharing Form. This should include the time and date of the footage requested; the reasons for the request; the justification for the disclosure; who it was disclosed to; the method of disclosure; the name of the decision maker and data of decision to disclose.
88. Internal disclosure requests will be assessed locally, but the Information Governance team will provide assistance responding to requests.

Freedom of Information Requests

89. Individuals are permitted to request CCTV footage under the Freedom of Information (FOI) Act 2000.
90. The Council's Complaints and Information Team coordinates FOI requests for the Council and will also coordinate any CCTV data required as part of a FOI. Exemptions under the FOI Act will continue to apply. In the majority of circumstances, all personal data will need to be redacted from footage requested under FOI.

Roles and Responsibilities

91. Responsibility for approving this procedure rests with the Information Governance Board. The approval of subsequent reviews will ordinarily be undertaken by the Procedures and Standards Sub-Group of the Information Governance Board. The Data Protection Officer (DPO) may approve minor amendments.

92. The Surveillance Camera Commissioner requires the Council to nominate a Senior Responsible Officer (SRO) to deliver a corporate approach to the organisation's responsibilities arising from the PoFA 2012. The SRO will ensure the integrity and efficacy of processes in place to enable compliance with The Protection of Freedoms Act and other relevant legislation. The Council's DPO will fulfil this role.
93. The DPO has overall responsibility for monitoring the implementation of this procedure and, with the support of the Information Governance Team, will ensure that a central record of all surveillance camera systems is maintained which includes details about the status of associated DPIAs.
94. The DPO and Information Governance Team will develop and provide relevant training for staff charged with owning and operating surveillance camera systems and will provide ongoing advice and support.
95. Information Asset Owners (Service Directors) are accountable for ensuring that surveillance camera systems operating as part of their directorate's business, do so in accordance with the provisions of this procedure. Specifically, they will:
 - a. Ensure that planning for any new Surveillance camera systems is informed by a DPIA and that the DPIA is approved before the system becomes operational.
 - b. Assign a Surveillance Camera System Owner to be responsible for the oversight of all new and existing systems. This maybe, but is not required to be, the Information Asset Owner (typically Group Manager) for the business area undertaking the surveillance or the Nominated Property Officer for a building.
96. The Surveillance Camera System Owner will be responsible for ensuring that this procedure and Surveillance Camera Codes of Practice is adhered to and will:
 - a. Ensure an approved surveillance camera DPIA is in place for each surveillance camera system under their ownership and notify the Information Governance Team (via data.protection@nottscc.gov.uk) prior to any change of use of the system or a change in system ownership.
 - b. Ensure appropriate signage and privacy information (where appropriate) is in place to inform individuals of the surveillance camera system
 - c. Ensure that there is a contract in place with the surveillance camera system supplier with appropriate data protection and privacy clauses and manage the surveillance camera system supplier in accordance with the [Surveillance Camera Commissioner's Code of Practice Owner/Installer Points for Consideration](#)
 - d. Nominate a system operator(s), where required, to be responsible for day-to-day operational use and ensure that they are trained to undertake their specific duties in relation to this role.
 - e. Put in place localised, system(s) specific operating procedures where appropriate to complement this corporate procedure.
 - f. Ensure regular reviews are conducted to provide ongoing assurance that the objectives of the surveillance camera system are being met and the operating procedures are operating effectively.

97. Responsibility for the implementation of this and associated procedures and for reporting performance issues related to surveillance camera systems rests with all employees who have involvement in the management of the surveillance camera equipment.

98. Staff who use the CCTV system have the following responsibilities:

- a. To uphold the arrangements of this procedure and associated Codes of Practice.
- b. To handle images and data securely and responsibly, within the aims of this Procedure.
- c. To be aware that they could be committing a criminal offence if they misuse surveillance camera images.
- d. To uphold the corporate procedure for subject access requests.
- e. To report any breach of procedure to using the [Council's data breach process](#)
- f. To attend training / refresher sessions as required.

Compliance with this Procedure

99. Wilful or negligent disregard for information governance policies and procedures will be investigated and may be treated as a disciplinary matter under the relevant employment procedure(s) which could lead to dismissal or the termination of work agreement or service contracts.

Review

100. This procedure will be regularly monitored and reviewed by the Data Protection Officer (or their nominee) who will revise it in line with any localised or wider learning in this field.

101. Beyond that, the procedure will be monitored and reviewed annually in line with legislation and codes of good practice.

Advice, Support & Further Information

102. Further advice about this procedure can be obtained from:

<p>Information Governance Team Email: data.protection@nottscc.gov.uk Telephone: 0115 8043800</p>	<p>Complaints & Information Team Email: accessto.records@nottscc.gov.uk Telephone: 0115 9772788</p>
--	--

103. Further reading and supporting information:

Title (as hypertext link) and publication date	Author
Surveillance Camera Code of Practice	Surveillance Camera Commissioner (SCC)
Self-Assessment Tools	SCC
Buyers Toolkit	SCC

Nottinghamshire County Council - Surveillance Camera (CCTV) Procedure

Passport to compliance - aimed primarily at public space CCTV systems	SCC
Surveillance Camera Code of Practice: A Guide for Councillors	SCC
In the picture: A data protection code of practice for surveillance cameras and personal information	Information Commissioner's Office (ICO)
Information Commissioner's Office Surveillance Webinar	ICO

Document Control

Owner	Caroline Agnew, Data Protection Officer
Author	Caroline Agnew, Data Protection Officer
Last Reviewer	Tim Boden, Information Governance Advisor
Approver	Data Protection Officer
Date of Approval	15/12/2021
Date of next review	01/12/2022
Version	2.7
Classification	Public

Version	Date	Changes
1.0	15/02/19	Original document approved by Information Governance Group.
2.0	25/03/19	Substantial rewrite to take account of various aspects of guidance and good practice and to address issues arising from CCTV related Data Protection Impact Assessments. Approved by Information Governance Board subject to business comments.
2.1	30/04/19	Minor revision to include comments from Gareth Johnson about responsibility for maintaining databases for cross-referencing. Approved by DPO.
2.2	28/06/19	Minor revision to include comments following JCNP meeting.
2.3	01/11/19	Minor revision to include details of evaluation process.
2.4	13/01/2020	Minor revisions to take account of comments from the Investigatory Powers Commissioners Office (IPCO) 23/12/2019; reference to holding data which is subject of a request; appendices embedded.
2.5	27/04/2020	Minor revision to include procedure for third party information disclosures which do not fit into the category of police requests or legal requests.
2.6	19/09/2020	Minor revision to amend retention period in line with a change to retention schedule.
2.7	15/12/2021	Addition of internal request procedure.

Appendix A

Data Protection Impact Assessment (DPIA) for Surveillance Camera Systems

This link takes you to the DPIA documents:

<https://www.gov.uk/government/publications/privacy-impact-assessments-for-surveillance-cameras>



The DPIA template is comprised of 2 levels, broken down into 6 areas:

1. Assessment of the need for the surveillance system
2. Definition of hardware, software and firmware, including camera types utilised
3. Location of cameras
4. Asset register
5. Privacy risks and mitigations
6. Information flows



The County Council's Information Governance Team (email data.protection@nottscc.gov.uk or telephone 0115 8043800) will provide advice on completing the DPIA.

Examples of Surveillance Camera System Signage

<p>Appropriate signage</p> <p>States purpose, who controls the system and how further information can be obtained.</p>	
<p>Inappropriate signage</p> <p>Does not state how further information can be obtained.</p>	

<p>Appendix C</p>	<p>NCC general CCTV Subject Access Request Form</p>	 <p>CCTV Subject Access Request Form.docx</p>
<p>Appendix D</p>	<p>Clayfields House Secure Children’s Home Subject Access Request Form</p>	 <p>CCTV Subject Access Request Form - Clayfi</p>

Nottinghamshire County Council - Surveillance Camera (CCTV) Procedure

Appendix E	Application for disclosure of surveillance camera images for the prevention, detection and prosecution of crime [Schedule 2, 2(1) of DPA 18]	 CCTV Disclosure under Sch2. 2 - Crime
Appendix F	Application disclosure of surveillance camera images in connection with legal proceedings or required by law [Schedule 2, 5(3) of DPA 18]	 CCTV Request Form Sch 2,5 - Legal Procee