October 2016

Policy for the operation of CCTV surveillance systems
on
Cheltenham Borough Council property

(Excluding CCTV systems operated by Gloucestershire Police in partnership with CBC)

CHELTENHAM
BOROUGH COUNCIL

Contents

Purpose

1.1. The purpose of corporate policy is twofold, firstly it will be to ensure that individuals and the wider communities have confidence that surveillance cameras are deployed to protect and support them, rather than spy on them.

1.2. The second purpose is to provide assurance that where Cheltenham Borough Council uses these complex technologies it will do so in line with the requirements for Data Protection Act 1998.

1.3. This Corporate CCTV Policy is approved by Cheltenham Borough Council's Cabinet. It provides guidance on the appropriate and effective use of surveillance camera systems and in particular how it meets the requirements of;

- The Human Rights Act 1998 article 8
- the Data Protection Act 1998. (1998 Act)
- the Regulation of Investigatory Powers Act 2000. (2000 Act)
- the Protection of Freedoms Act 2012. (2012 Act)
- Information Commissioners CCTV Code of Practice
- Surveillance Commissioners, Surveillance Camera Code of Practice.
- Data Protection Policy
- guidance and processes in relation to the Regulation of Investigatory Powers Act (RIPA)

1.4. Any system operator (Service Manager) who has the responsibility for a CCTV scheme must have a scheme specific Code of Practice in place before it becomes operational or within 6 months of the approval of this document.

1.5. The purpose of this Corporate Policy is to provide guidance to Service Managers who are the CCTV operators on the management, administration and operation of system. To enable them to agree and publish a system specific Code of Practice for their service area i.e. car parks, public buildings.

1.6. It will assist system owners, management and operators of the systems to understand their legal and moral obligations whilst reassuring the public about the safeguards contained within it.

1.7. The System owners (Service Manager) of the CCTV systems shall be required to give a formal undertaking through the Annual Assurance review that they comply with the CCTV Policy and their Code of Practice and act in good faith with regard to the basic principles contained within it.

1.8. The system operator (Service Manager) is responsible for compliance with the requirements of the Data Protection Act.

1.9. Any major changes to this Code of Practice will be approved by Cabinet. This Code of Practice will be subject to review as required by the Director of Resources who is authorised to make minor amendments.

1. **DEFINITIONS to be used in all system specific Codes of Practice**

1.1. **CCTV system** means "Surveillance camera systems" has the meaning given by Section 29(6) of the 2012 Act and is taken to include:

a. closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems;

b. any other systems for recording or viewing visual images for surveillance purposes;

c. any systems for storing, receiving, transmitting, processing or checking the images or information obtained by (a) or (b);

d. any other systems associated with, or otherwise connected with (a), (b) or (c).

1.2. **CCTV control and monitoring facility** shall mean the area of a building or land where CCTV is monitored and data recorded, retrieved and analysed.

1.3. **CCTV scheme** shall mean all of the arrangements for closed circuit television in the service area and is not limited to the technological system, staff and operational procedures.

1.4. **CCTV Code of Practice (service specific) systems** means that if Service manager considers that there may be a need for a CCTV system, they will need to carry out an assessment based upon the two model codes of practice (Information Commissioner and CCTV Surveillance Commissioner) and the advice in this document prior to its installation.

1.5. **Data** shall mean all information, including that about a person in the form of pictures, and any other associated linked or processed information.

1.6. **Data Controller is** Cheltenham Borough Council. and is responsible for determining the purposes for which and the manner in which any personal data are, or are about to be processed.

1.7. **Overt Surveillance** (any surveillance that is obvious to the subject)

1.8. **Objectives.** The overall objective of this policy is to ensure that the Council complies with all relevant legislation and to provide support and guidance to System managers so that they can undertake Privacy Impact Assessments, Needs Analysis and develop service specific CCTV Codes of Practice. This in turn will support the principle that the community at large should be satisfied that the public CCTV systems are being used, managed and controlled in a responsible and accountable manner.

1.9. **Personal Data** means data which relates to a living individual who can be identified:
- From that data, or
- From that data and other information which is in the possession of or is likely to come into the possession of, the data controller.

1.10. **Public place** has the meaning given by Section 16(b) of the Public Order Act 1986 and is taken to include any highway and any place to which at the material time the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission.

1.11. **Processing** means obtaining, processing, recording, deleting or holding the information or data or carrying out any operation or set of operations on the information or data. The full definition is explained in Part 1, Section 1 of the Data Protection Act 1998[1].

[1] http://www.legislation.gov.uk/ukpga/1998/29/section/1

1.11. **Retrieval System** means the capability, in any medium, of effectively capturing data that can be retrieved, viewed or processed.

1.12. **Sensitive Personal Data** is personal data which is deemed to be sensitive in clause 2 of the Data Protection Act 1998. For example;

- the commission or alleged commission of any offences
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

1.13. **System Operators** are Service managers.

1.14. **Recording Material** means any medium that has the capacity to store data and from which data can later be recalled irrespective of time.

1.15. **Roles and Responsibilities** (to be defined within all system specific Codes of practice)

1.16. **The System Owner** (service manager), shall be responsible for the system code of practice covering the effective management and public relations of the scheme in respect of the operation within their service area.

1.17. They shall produce a code of practice for their CCTV system and be responsible for its implementation. This shall be carried out in consultation with users of the syetem and provide for the release of information relating to the operation of the it. Any complaints will be dealt with in line with the agreed corporate complaints policy and procedure.

1.18. **The System Manager** (may also be the Service manager) or designated member of staff should undertake regular reviews of the documented procedures to ensure that the provisions of this Code are being complied with. The System Manager should retain responsibility for the implementation of procedures to ensure that the system operates according to the purposes for which it was installed and in accordance with the objectives identified for the system. The System Manager shall also ensure that on a day-to-day basis all equipment is working correctly and that all staff comply with the Code of Practice and any procedures.

1.19. **Operators -** The system will be utilised according to operational needs and the operators of the system will be authorized staff employed at the specific location a. Operators will be responsible for complying with the code of practice and procedural manual. They have a responsibility to respect the privacy of the individual, understand and comply with the objectives of the scheme. The information recorded must be accurate, adequate and relevant to the purpose of the scheme.

1.20. **Users –** System Users are all those people who legitimately have access to recorded data and equipment but are not covered within the other defined roles and responsibility sections of this policy.

1.21. **Audit** Regular Internal audits will check the operation of the scheme and the compliance with the code of practice. It will consider the following:

- The level of attainment of objectives and procedures
- Random audits of the data log and release of information
- Standard costs for the release of viewing of material
- The complaints procedure.

Introduction

1.22. Surveillance camera systems are deployed extensively within Cheltenham; these systems are valuable tools which contribute to public safety and security and in protecting both people and property.

1.23. Cheltenham Borough Council supports the individual's right to privacy and will insist that all agencies involved in the provision and use of public CCTV systems owned by the Council accept this fundamental principle as being paramount.

1.24. In addition to the need to manage the system correctly for its intended purpose the Council also has to ensure that it complies with the requirements of the Data Protection Act 1998

Part 1 Surveillance

The use of the CCTV and ANPR systems for Overt Surveillance

1.25. Cheltenham Borough Council needs to achieve an appropriate balance between public protection and individual privacy.

1.26. The government considers that wherever overt surveillance in public places is in pursuit of a legitimate aim and meets a pressing need, any such surveillance should be characterised as surveillance by consent, and such consent on the part of the community must be informed consent and not assumed by a system operator.

1.27. To help it achieve overt surveillance by consent the Council has adopted the Surveillance Commissioners single set of guiding principles that are applicable to all surveillance camera systems in public places.

1.28. By following these guiding principles it allows the Council to establish a clear rationale for any overt surveillance camera deployment in public places, to run any such system effectively and helping it to ensure compliance with other legal duties.

Guiding Principles

1.29. The Surveillance Camera Commissioner code sets out guiding principles that should apply to all surveillance camera systems in public places. CBC have adopted these principles in full to provide a framework for its system operators and users of surveillance camera systems so that there is proportionality and transparency in their use of surveillance, and systems are capable of providing good quality images and other information which are fit for purpose.

The Surveillance Commissioners, Surveillance Camera Code of practice which helps system operators consider the guiding principles.

1.30. The 12 guiding principles are:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

1.31. **The use of the CCTV and Automated Number Plate Recognition (ANPR) systems for covert surveillance**

1.32. Covert Surveillance by public authorities (as defined in Part II of the 2000 Act) is not covered by this code but is regulated by the 2000 Act. and the Councils RIPA guidance.

1.33. Any such covert use of private systems by or on behalf of a public authority (with the authority's knowledge) immediately places such use within the bounds of the 2000 Act.

1.34. Should there be a need to consider the use of the system for covert purposes then advice must be sought from the RIPA Senior Responsible Officer as defined in the CBC RIPA Guidance and One Legal.

1.35. The use of ANPR system in general

1.36. The Council uses ANPR systems within its Regent Arcade car park and may introduce and use that technology at other car parks in the future.

1.37. The use of technologies such as ANPR that rely on the accuracy of information generated elsewhere such as databases provided by others should not be introduced without regular assessment to ensure the underlying data is fit for purpose.

1.38. The system operator will have a clear policy to determine the inclusion of a vehicle registration number or a known individual's details on the reference database associated with such technology. A system operator should ensure that reference data is not retained for longer than necessary to fulfil the purpose for which it was originally added to a database.

1.39. There may be occasions when the inclusion of information about an individual in a reference database with the intention of undertaking surveillance can be considered as Covert Surveillance and thus fall with the bounds of the 2000 Act.

1.40. Where the system is operated by a third party on behalf of the council, the System Owner will ensure that all of the measures that would be applied to system operated by it are applied. Compliance will be monitored by Internal Audit.

1.41. CCTV in the workplace

1.42. When you install CCTV in a workplace, such as an office, it is likely to capture pictures of employees, even if they are not the main subject of surveillance. If the purpose of the CCTV is solely to prevent and detect crime, then you should not use it for monitoring the amount of work done or compliance with company procedures.

1.43. You may get requests to disclose information captured by the CCTV system from employees or HR GoSS because of on-going disciplinary action, disclosure should only be made if this is consistent with the registered purpose for the system. Any request for the disclosure of information should be made to the Customer Relations Manager on the approved Subject Access request form

1.44. In some cases, it may be appropriate to install CCTV specifically for workforce monitoring. You should go through the decision making process in section 4 of the Information Commissioners code, take advice from HR GoSS and consider whether it is justified. In particular, consider whether better training or greater supervision would be a more appropriate solution

1.45. Any overt monitoring of any employee using CCTV can only be done with the consent of the Director and after consultation with HR GoSS

1.46. The covert monitoring of employees must not take place unless it has been specifically authorised in advance using the codes of practice, guidance and procedures under The Regulation of Investigatory Powers Act 2000

Part 2 Data Protection Act

2.1. If System Operators have followed the advice of the Surveillance Commissioners surveillance camera code of practice, then many of the issues relating to privacy and data protection will already have been covered.

2.2. However System Operators also need to have taken into account how they are going to store, collect, share, manage and protect the data that it has collected.

2.3. This Information Commissioners office (ICO) code of practice provides good practice advice for those involved in operating CCTV and other devices which view or record images of individuals. It also covers other information derived from those images that relates to

individuals (for example vehicle registration marks). The Information Commissioners Office provides a checklist to help you assess the need and operation of any CCTV system

2.4. The DPA not only creates obligations for organisations, it also gives individuals rights, such as the right to gain access to their details and to claim compensation when they suffer damage.

2.5. The basic legal requirement is to comply with the DPA itself. To support this right to privacy the Council agreed a Data Protection Policy that provides guidance and advice on the collection, storage and management of data. This applies equally to any data collected through CCTV systems

2.6. This code sets out the Information Commissioner's recommendations by following them it will:
help ensure that those capturing images of individuals comply with the DPA;

mean that the images that are captured are usable; and

reassure those whose images are being captured.

The Information Commissioners Office provides a checklist to help you assess the need and operation of any CCTV system

Appendix A
The Systems Code of practice should include information on;

1.1. **Management of the schemes**

1.2. A risk assessment must be carried out to assess the need and requirements of CCTV systems within individual service locations. The cameras must therefore be sited to capture images which are relevant to the purposes for which the schemes have been established. This risk assessment is reviewed on an annual basis by Service Managers.

1.3. Details of the cameras that have been sited to capture images which are relevant to the purpose for which the scheme has been established.

1.4. Details of how the scheme will be operated fairly, within the applicable law and only for the purposes for which it is established or which are subsequently agreed in accordance with the Code of Practice.

1.5. The owners, users and any visitors to the control, monitoring and recording facilities will be required to sign a formal confidentiality declaration that they will treat any viewed and/or written material as being strictly confidential and that they undertake not to divulge it to any other person.

1.6. Those who have authorised access are aware of the purpose(s) for which the scheme has been established and that the CCTV equipment is only used to achieve the identified purposes.

1.7. Scheme and Signage

1.8. The CCTV scheme aims to provide surveillance of the public areas within the specified location, in order to fulfil the purposes of the scheme. The area protected by CCTV will be indicated by the presence of signs. The signs will be placed so that the public are aware before they enter a zone which is covered by surveillance equipment. The signs will state the organisation responsible for the scheme, the purposes of the scheme and a contact telephone number.

1.9. Data will not be held for longer than necessary and disposal of information will in accordance with retention schedules and disposal policies. It is important that disposal of records happens as part of a managed process and is adequately documented within the service document retention schedule.

1.10. Point of contact

1.11. Any scheme Code of Practice should inform the public on how to make contact with the owners of the scheme it should specify the location of the equipment e.g. Municipal Building, North Place Car Park etc. and who to write to for additional information.

1.12. Release of information to the public

1.13. Information can be released to justifiable third parties who can show legitimate reasons for access. They will be required to request any information with reasons in writing and identify themselves.

Information will be released if the reasons are deemed acceptable and complies with the principles of the Data Protection Act.

1.14. Individuals may request in writing to view information concerning them held on record in accordance with the Data Protection Act 1998. System managers will need to consider if there are any other third parties within the images being requested and consider redacting any third part data

1.15. Information on how to obtain an application form can be found on Cheltenham Borough Council web site www.cheltenham.gov.uk or by writing to Customer Relations (section 4.4 for details).

1.16. Release of information to statutory prosecuting bodies

1.17. The policy is to assist statutory prosecuting bodies such as the Police, and statutory authorities with powers to prosecute and facilitate the legitimate use of the information derived from the scheme. Service managers need to ensure that any system will meet the requirements of any prosecuting body i.e. HD quality cameras.

1.18. Statutory bodies may have access to information permitted for disclosure on application to the System Owner or the System Manager; these applications must be in writing, provide the reasons, statement of purpose and meet the requirements of the Data protection Action.

1.19. System Registration

1.20. The Council must be registered with the Information Commissioner's Office (ICO) to process personal data, and it is the responsibility of service managers to ensure that this is kept up to date in respect of their service area. Any new schemes and amendments to a scheme that result in the need to update the ICO register must be forwarded to the Customer Relations Team.

1.21. Accountability

1.22. Cheltenham Borough Council supports the principle that the community at large should be satisfied that the public CCTV systems are being used, managed and controlled in a responsible and accountable manner and that in order to meet this objective there will be independent assessment and scrutiny.

1.23. Complaints - A member of the public wishing to make a complaint about the system may do so through the Cheltenham Borough Council complaints procedure (see section XXX . for details of how to contact Customer Relations)

1.24. Codes of Practice - A copy of the Code of Practice will be made available to anyone on request by contacting the CCTV system owner i.e. the Service Manager for that specific system,

1.25. CCTV Control Management And Operation

1.26. Access to the monitoring and recording areas will be strictly controlled.

1.27. The System Manager or in his/her absence the Deputy, is authorised to determine who has access to the monitoring area. This will normally be:

- Authorised Personnel
- Police officers requiring to view a particular incident, or intelligence or evidential purposes. These visits will take place by prior appointment.

- Engineers and cleaning staff (These people will receive supervision throughout their visit)

1.28. Inspectors/Auditors may visit the monitoring and recording facility without prior appointment.

1.29. All visitors to the monitoring and recording area, including Police Officers, will be required to sign a visitors log and a declaration of confidentiality.

1.30. Observation and recording of incidents

1.31. Recording will be throughout the 24 hour period. The system will be monitored on the basis of operational necessity.

1.32. Access to recorded images

1.32. Access to recorded images will be restricted to the manager or designated member of staff who will decide whether to allow requests for access by third parties in accordance with the disclosure policy. Those requests must be in writing on the Subject Access request form. See paragraph 1.42 in relation to requests made by employees.

1.34. Privacy And Disclosure Issues

1.35. The following principles must be adhered to:

1.36. All employees will be aware of the restrictions set out in this Code of Practice in relation to access to, and disclosure of, recorded images

1.37. Images not required for the purposes of the scheme will not be retained longer than necessary

1.38. Monitors displaying images from areas in which individuals would have an expectation of privacy will not be viewed by anyone other than authorised persons

1.39. Recorded material will only be used for the purposes defined in the objectives and policy

1.40. Access to recorded material will be in accordance with policy and procedures

1.41. Information will not be disclosed for commercial purposes and entertainment purposes

1.42. All access to the medium on which the images are recorded will be documented

1.43. Access to recorded images will be restricted to those staff who need to have access in order to achieve the purpose(s) of using the equipment

1.44. Viewing of the recorded images should, where possible take place in a restricted area.

1.45. Recorded Material Management

1.46. Images that are not required for the purpose(s) for which the equipment is being used will not be retained for longer than is necessary. The detail as to how long data should be held will be defined within the service retention schedule. While images are retained access to and security of the images will be controlled in accordance with the requirements of the Data Protection Act.

1.47. Recorded material should be of high quality. In order for recorded material to be admissible in evidence total integrity and continuity must be maintained at all times.

1.48. Security measures will be taken to prevent unauthorised access to, alteration, disclosure, accidental loss or destruction of recorded material.

1.49. Recorded material will not be released to organisations outside the ownership of the system other than for training purposes or under the guidelines referred to previously.

1.50. Images retained for evidential purposes will be retained in a secure place where access is controlled.

1.51. The system records features such as the location of the camera and/or date and time reference and documented procedures are in place for ensuring accuracy.

1.52. Quality, in order to ensure that clear images are recorded at all times the equipment for making recordings will be maintained in good working order with regular servicing in accordance with the manufacturer's instructions.

1.53. Recorded Material Register

1.54. There will be a register documenting the access to recorded media.

1.55. Documentation

1.56. Log books must be sequential in order that pages or entries cannot be removed and full and accurate records kept.

1.57. The following Administrative documents shall be maintained:

- media tracking register
- occurrence/incident book
- visitors register
- maintenance of equipment, whether routine or breakdown
- list of installed equipment