

BS 7958:2015



BSI Standards Publication

Closed circuit television (CCTV) – Management and operation – Code of practice

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2015

Published by BSI Standards Limited 2015

ISBN 978 0 580 86308 0

ICS 13.310; 13.320; 33.160.40

The following BSI references relate to the work on this document:

Committee reference GW/3

Draft for comment 15/30299657 DC

Publication history

First published as BS 7958, December 1999

Second edition, December 2005

Third edition, September 2009

Fourth (present) edition, August 2015

Amendments issued since publication

Date	Text affected
------	---------------

Contents

Foreword *ii*

Introduction *iii*

1	Scope	1
2	Normative references	1
3	Terms and definitions	2
4	Principles and management of a CCTV scheme	4
5	Personnel	12
6	CCTV control centre	13
7	Incident handling	14
8	Privacy and disclosure issues	15
9	Recorded material management	17
10	Documentation	20

Annexes

Annex A (informative) Surveillance Camera Code of Practice – 12 guiding principles 22

Annex B (informative) Data Protection Act 1998 – 8 guiding principles 23

Annex C (normative) Contractor responsibilities within BS 7958 24

Annex D (normative) Management and operation of CCTV traffic enforcement cameras 26

Annex E (normative) Contracted remote CCTV control centre responsibilities within BS 7958 33

Bibliography 36

List of figures

Figure D.1 – Example of CCTV image receiving centre log sheet 29

Figure D.2 – Example of occurrence log 30

List of tables

Table A.1 – 12 guiding principles of the Surveillance Camera Code of Practice 22

Table B.1 – 8 guiding principles of the Data Protection Act 1998 23

Summary of pages

This document comprises a front cover, an inside front cover, pages i to iv, pages 1 to 38, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 31 August 2015. It was prepared by Technical Committee GW/3, *Manned security services*. A list of organizations represented on this committee can be obtained on request to its secretary.

Supersession

This British Standard supersedes BS 7958:2009, which is withdrawn.

Information about this document

This is a full revision of the standard, which has been updated to reflect current practice.

Use of this document

As a code of practice, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this British Standard is expected to be able to justify any course of action that deviates from its recommendations.

Presentational conventions

The provisions of this standard are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is “should”.

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

The word “should” is used to express recommendations of this standard. The word “may” is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word “can” is used to express possibility, e.g. a consequence of an action or an event.

Notes and commentaries are provided throughout the text of this standard. Notes give references and additional information that are important but do not form part of the recommendations. Commentaries give background information.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

Introduction

Closed circuit television (CCTV) schemes that process personal data are obliged to conform to certain legislation, most importantly the Data Protection Act 1998 (DPA) [1], the Human Rights Act 1998 (HRA) [2], the Freedom of Information Act 2000 [3], the Protection of Freedoms Act 2012 [4] and the Regulation of Investigatory Powers Act 2000 [5]. This British Standard is designed to supplement that legislation and aims to ensure fairness, purpose and responsibility.

Attention is also drawn to the Private Security Industry Act 2001 [6], which contains provisions for regulating the private security industry. A person falling within the definition of providing security industry services under the Private Security Industry Act 2001 [6] is required to be licensed in accordance with that Act.

Monitoring for traffic offences does not require a SIA (Security Industry Authority) Licence. However, if operators monitoring for traffic offences, who are employed by organizations providing the service under contract, provide an additional security service involving use of CCTV then they are required to hold the SIA CCTV (Public Space Surveillance) Operator Licence prior to being deployed in contractual security work.

Attention is drawn to the Surveillance Camera Code of Practice [7] and its 12 guiding principles, which are applicable to public space CCTV systems.

Irrespective of the ownership, this British Standard covers CCTV schemes used in areas where the public have a "right to visit". These areas include, but are not limited to:

- a) a place that is privately owned, but where the public perceive no boundary;
- b) a place where a public service is offered;
- c) public footpaths, roads, bridle-ways, etc.;
- d) educational establishments and hospitals;
- e) sports grounds where access is unrestricted, supermarkets and housing areas; and
- f) public arenas such as sports stadiums and public places where events are held as an alternative to regular activities in those locations.

1 Scope

This British Standard gives recommendations for the management and operation of CCTV within a controlled environment, where data that might be offered as evidence are received, stored, reviewed or analysed. This standard applies to the monitoring and management of public spaces, including automatic number plate recognition (ANPR) and traffic enforcement cameras.

For control rooms whose operation falls within the scope of BS 7499, BS 5979 or BS 8591, all of the security requirements, both physical and procedural, of the relevant British Standard remain applicable.

This British Standard is applicable to CCTV schemes used in public places such as the following:

- a) areas where the public are encouraged to enter or have a right to visit, such as town centres, shopping malls, public transport, health establishments;
- b) schemes that overlook a public place, such as traffic monitoring and traffic enforcement schemes; and
- c) private schemes where a camera view includes a partial view of a public place.

This British Standard also provides good practice for all other CCTV schemes.

This British Standard takes due regard of the 12 guiding principles of the Surveillance Camera Code of Practice [7] (see Annex A) and the Information Commissioner's *CCTV Code of practice* [8] and the Data Protection Act 1998 [1] principles (see Annex B).

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 5979, *Remote centres receiving signals from fire and security systems – Code of practice*

BS 7499, *Static site guarding and mobile patrol service – Code of practice*

BS 7858, *Security screening of individuals employed in a security environment – Code of practice*

BS 8591, *Remote centres receiving signals from alarm systems – Code of practice*

BS EN 15713, *Secure destruction of confidential material – Code of practice*

BIP 0008-1, *Evidential weight and legal admissibility of information stored electronically – Code of practice for the implementation of BS 10008*

BIP 0008-2, *Evidential weight and legal admissibility of information transferred electronically – Code of practice for the implementation of BS 10008*

BIP 0008-3, *Evidential weight and legal admissibility of linking electronic identity to documents – Code of practice for the implementation of BS 10008*

3 Terms and definitions

For the purposes of this British Standard, the following terms and definitions apply.

3.1 CCTV control centre

secure central location for a CCTV scheme, where images are collected, used, disclosed, retained or disposed of

3.2 CCTV scheme

totality of arrangements for CCTV in a locality including, but not limited to, the technological system, staff and operational procedures

3.3 CCTV system

surveillance items comprising camera and associated equipment for monitoring, transmission and controlling purposes

NOTE A whole system is not limited to equipment sited at one locality. It can include systems that use dial-in dial-out, remote transmission or decentralized control.

3.4 clean tape

tape which has either been degaussed not more than 12 times, or is new

3.5 contractor

party contracted by the owner to undertake agreed services

3.6 controlled environment

location in which data that might be offered as evidence are received, stored, reviewed or analysed, including at the CCTV control centre

3.7 customer

individual or body retaining the services of an organization

3.8 data

all information, including that about a person

NOTE In CCTV systems, this includes pictures, sound and any other associated, linked or processed information.

3.9 evidence copy

copy taken from the master copy with a clear audit trail which is offered as evidence

3.10 hard copy print

paper copy of an image or images that already exist on recorded material

3.11 incident

activity that warrants a response

3.12 local procedures

documents relating to the processing of aspects of the CCTV scheme

3.13 manager(s)

person or persons designated and trained as having direct responsibility for the implementation of the policies, objectives and methods of control of a CCTV scheme, as defined by the owner of the scheme

3.14 master copy

first copy to be produced, that is designated and documented as such and then stored securely pending its production (if required) at court as an exhibit

NOTE All use and movement of the master copy is logged in an audit trail.

3.15 monitoring period

length of time during which monitoring is carried out as defined by local procedures

3.16 operator

person specifically designated and authorized by the owner of a CCTV scheme to carry out the physical operation of controlling that scheme

3.17 operator's log

record, including date and time, for a workstation that also includes details of any events, plus details of activities such as maintenance and use

3.18 organization

sole or principal provider of CCTV monitoring services to a particular customer

3.19 owner

legal person or entity, agency or individual designated as having overall responsibility for the formulation and implementation of the policies, objectives and control of a CCTV scheme

NOTE 1 The owner also has responsibility for all statutory responsibilities, including the role of "data controller" (see the Data Protection Act 1998 [1]).

NOTE 2 The owner could be a partnership, provided it has a formal constitution.

3.20 privacy impact assessment

assessment of the impact a CCTV system has on an individual's right to privacy

NOTE Attention is drawn to the Human Rights Act 1998 [2] and the Data Protection Act 1998 [1]. Further guidance can be found in the Information Commissioner's Conducting privacy impact assessments code of practice [9].

3.21 process

obtaining, recording or holding information or data or carrying out any operation or set of operations on the information or data

NOTE This definition is taken from the Data Protection Act 1998 [1].

3.22 recorded material

any data recorded on any medium that has the capacity to store data

3.23 recording material

any medium that has the capacity to store data and from which data can later be recalled, irrespective of time

3.24 recordings

electronic capture of images or data

3.25 remote centre

location remote from the supervised premises, in which the information concerned with the state of one or more alarm systems is collected either for reporting or for onward transmission

3.26 secure storage

lockable cabinet, container or room located within the CCTV control room or the building which houses the CCTV control room and to which access is restricted to those persons authorized by the owner or supervisor

3.27 staff

personnel involved in the management and operation of CCTV

3.28 supervisor

person designated and trained to ensure the required operation of the CCTV scheme and to meet any procedural instruction issued by the owner or manager

3.29 temporary systems

mobile and remote systems which are part of the main CCTV scheme

3.30 working copy

copy of recordings which is used for review

NOTE Also referred to as the "slave copy".

4 Principles and management of a CCTV scheme

4.1 Objectives

4.1.1 Use

The objectives of a CCTV scheme should have a clearly defined purpose or purposes in pursuit of a legitimate aim. The data held should be appropriate for those objectives and the owner should have reasonable cause to hold the data. The purpose or purposes should be clearly documented against which the ongoing use of the system and any images or other data can be assessed.

NOTE 1 Attention is drawn to Principle 1 of the Surveillance Camera Code of Practice [7] and Principle 2 of the Data Protection Act 1998 [1].

NOTE 2 Many CCTV schemes have developed ancillary public information outputs that do not relate directly to an individual. The extended use of such schemes is aimed at improving public information and confidence and does not compromise non-disclosure. The following are some examples:

- *availability of car parking relayed to local radio or the internet;*
- *traffic congestion reports, local radio, phone-in or answer service; and*
- *public awareness, crime watch (vulnerable areas monitored actively to allay public concern about safety and enable a swift response to incidents).*

4.1.2 Effectiveness

A CCTV scheme should capture, process, analyse and store images and data at a quality which is suitable for its defined purpose. The data or images should not be held for longer than necessary in accordance with the scheme's objectives.

NOTE 1 For example, recording sound in a public place where a conversation might be private might not be appropriate.

Where the purpose of the CCTV scheme includes crime prevention, detection and investigation, it should be capable of delivering images and other data which are of evidential value to the criminal justice system. Effective safeguards should be put in place to ensure the forensic integrity of recorded images and data including meta data (e.g. time, date location) are recorded reliably and any data compression does not compromise the data below the quality required to meet the defined purpose. A record should be kept as an audit trail of how images and data have been handled if they are likely to be used as exhibits for the purpose of criminal proceedings in court.

NOTE 2 Attention is drawn to Principle 11 of the Surveillance Camera Code of Practice [7] and Principles 3 and 4 of the Data Protection Act 1998 [1].

4.1.3 Transparency

COMMENTARY ON 4.1.3

Surveillance by consent is dependent on the system operator being transparent and accountable.

Measures should be taken so that persons who are being monitored are made aware that such activity is taking place, who is undertaking the activity and the purpose of the activity; this is an integral part of overt surveillance and is a legal obligation.

In the development or review of a CCTV scheme, consultation and engagement are an important part of assessing whether there is a pressing need and a CCTV system is a proportionate response; consultation should be undertaken with all relevant parties and partners.

NOTE Attention is drawn to Principle 3 of the Surveillance Camera Code of Practice [7] and Principle 6 of the Data Protection Act 1998 [1].

4.1.4 Standards

Where appropriate, system operators should base their policies and procedures around approved standards.

NOTE 1 These can apply to not only the design, installation, operation and maintenance of the CCTV system, but also where applicable to any additional standards which cover advanced capabilities such as ANPR, body-worn video, facial recognition and video analytics.

NOTE 2 Attention is drawn to Principle 8 of the Surveillance Camera Code of Practice [7].

4.2 Policy

4.2.1 General

A CCTV scheme should have written policy statements which should include:

- a) a policy regarding the release of information to statutory prosecuting bodies;
- b) a policy regarding the release of information to members of the public who can show legitimate requirements for obtaining the information. The policy should include:
 - 1) the name and official address of the owner of the scheme;
 - 2) contact details for enquires;
 - 3) the objectives and policy of the scheme; and
 - 4) how to make a complaint.

- c) a policy or policies regarding the safety and integrity of the scheme. This should cover the physical security of the system, the IT security and resilience of the system and the vetting and training of staff using the system; and
- d) a complaints policy.

These policies should reflect best practice and should be regularly reviewed.

NOTE Attention is drawn to Principle 5 of the Surveillance Camera Code of Practice [7] and Principle 5 of the Data Protection Act 1998 [1].

4.2.2 Policy and scheme review

Regular reviews should be undertaken, at least annually, to ensure that the scheme still meets the specified purpose and to minimize the effects on individuals and their privacy.

The review should take account of, as a minimum, the following:

- a) whether the objective statements remain valid;
- b) changes to the scope of the scheme;
- c) contracts with suppliers;
- d) a review of the current data protection and legal requirements;
- e) a maintenance schedule and performance test of the CCTV system;
- f) the annual report and statistics; and
- g) the election of board members, if appropriate.

If the objectives of the scheme change then the CCTV system should be reviewed. If the objectives of the scheme are no longer valid, then the CCTV system should be withdrawn.

NOTE Attention is drawn to Principles 2 and 11 of the Surveillance Camera Code of Practice [7] and Principles 4 and 5 of the Data Protection Act 1998 [1].

4.3 Procedures

4.3.1 General

Responsibility and accountability for all CCTV system activities should be clearly set out, and management and reporting functions should be regularly reviewed and audited.

NOTE 1 Attention is drawn to Principle 4 of the Surveillance Camera Code of Practice [7] and Principle 7 of the Data Protection Act 1998 [1].

Where a CCTV system is used for more than one purpose (for example, crime prevention and detection and also for traffic management), those accountable for each purpose should be identified to facilitate effective joint working and decision making.

The administrative procedures to manage a CCTV scheme should be clearly set out. A procedural manual should be written to cover management and reporting functions, based on the objectives and principles contained within this British Standard. The type of system should be defined (e.g. observation or retrieval). Procedural functions to be covered should include:

- a) administration;
- b) staffing;
- c) communication;
- d) documentation;

- e) control room operations;
- f) access and security screening;
- g) data handling and data security;
- h) observation and incident protocol;
- i) maintenance and faults; and
- j) examples of standard forms.

Each procedure should clearly identify the following.

- 1) *Documentation*. The procedures by which the objectives and policies are upheld should be defined. These may be in written or electronic format but should be available at all times for reference by staff. The method by which operational procedures are changed should be clearly defined.
- 2) *Responsibilities*. The responsibilities of the owners and/or partners, managers, contractors and staff should be stated. A tiered structure should be defined that maps the operational role for all personnel involved in the scheme. This should include a response recommendation or guidance notes when handling matters relating to law and when working with the public, law enforcement agencies or other agencies. Relevant information on procedures covering investigation, complaints, non-disclosure and disciplinary measures should be included, together with procedures for redress.

NOTE 2 Attention is drawn to Principle 5 of the Surveillance Camera Code of Practice [7] and Principle 6 of the Data Protection Act 1998 [1].

4.3.2 Information security

Policies and procedures should be designed to ensure that any images or data are protected from unauthorized access and retained only until the purpose they have been retained for has been met, after which they should be destroyed. Retention lengths vary due to the purpose of the system but should be proportionate. These timescales should be reviewed on a regular basis in the light of changes to the aims and purpose of the system and in the light of experience.

The CCTV scheme should have regard for the physical security of equipment used to store and process images and data. It should also have regard for IT security to ensure that unauthorized access is denied unless the user has the appropriate access level. Each scheme needs to build policies and procedures in terms of both physical and IT security to secure the data being held. These should be reviewed on a regular basis.

NOTE Attention is drawn to Principles 6 and 9 of the Surveillance Camera Code of Practice [7] and Principles 7 and 8 of the Data Protection Act 1998 [1].

4.3.3 Access to data

Policies and procedures should be created to ensure that access to recorded images and stored data is restricted. These should also define who can gain access and under what circumstances access is approved and by whom.

NOTE 1 Access to images and data may be provided where permitted by legislation, for example where non-disclosure would be likely to prejudice the prevention and detection of crime or for national security purposes or where disclosure is authorized by a court of competent jurisdiction. There might be other limited reasons where disclosure of images to a third party is appropriate. Attention is drawn to the Data Protection Act 1998 [1], particularly Principle 6.

Policies and procedures should be in place to meet requests from individuals about images of themselves to manage those images where third parties are included. In addition there should be policies and procedures to deal with requests from public bodies for data information.

The owner should not disclose data without a record of the request and the authorization, which should be retained for a minimum period of 2 years.

NOTE 2 Attention is drawn to the Freedom of Information Act 2000 [3] and Principle 7 of the Surveillance Camera Code of Practice [7].

4.3.4 Supporting data

Where data collected by a CCTV scheme are to be used to provide meta data (for example vehicle registration numbers from ANPR cameras or face recognition), the accuracy of information generated or provided from elsewhere such as databases should be regularly assessed to ensure that such data are fit for purpose.

Reference data should only be retained for as long as necessary to fulfil the legitimate aims of the scheme.

The inclusion of personal information from a reference database might be deemed to be covert surveillance; policies and procedures to identify when this might be the case and methods to manage surveillance should be implemented in schemes where this is appropriate.

NOTE Attention is drawn to the Regulation of Investigatory Powers Act 2000 [5], Principles 7 and 12 of the Surveillance Camera Code of Practice [7] and Principles 4 and 5 of the Data Protection Act 1998 [1].

4.3.5 Use of temporary systems within the scheme

Where temporary systems are used within the scheme, the following should be stated, where applicable:

- a) the policy on notification of the use of temporary CCTV systems; and
- b) whether the limits of control are dictated by agreement with the police or other agencies.

4.3.6 Annual report

An annual report should be prepared for CCTV schemes monitoring public spaces. This report should be made available to the public.

NOTE 1 It might not be necessary for other CCTV schemes to produce an annual report.

The report should include the following details:

- a) a description of the scheme and the geographical area(s) of operation;
- b) the scheme's policy statement;
- c) the objective and scope of the scheme;
- d) any changes to the operation or management of the CCTV scheme;
- e) any changes that have been made to the policy;
- f) any proposals to expand or reduce the operation of the scheme; and
- g) the scheme's aims and objectives for the next 12 months.