BS 7958:2015

BSI Standards Publication

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

bsi.

...making excellence a habit.™

Publishing and copyright information

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

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This British Standard supersedes BS 7958:2009, which is withdrawn.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

This page deliberately left blank

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.

The report should also provide details of the scheme's achievements during the previous 12 months, which might be based on information already held by the scheme. The details of the scheme's performance should include:

1) the number of incidents recorded by the scheme;
2) the number of incidents reported to the law enforcement agencies and, where appropriate, other bodies, e.g. the local authority;
3) an assessment of the scheme's impact on crime levels and types of crime in the area covered by it; and
4) an assessment of the scheme's impact on its objectives, including:
   - the number of privacy impact assessments completed;
   - the number of reviews of footage by police and authorized agencies; and
   - the number of incidents per camera for the previous twelve months.

NOTE 2 Attention is drawn to Principle 10 of the Surveillance Camera Code of Practice [7].

4.3.7 Audit

An independent audit should be carried out to monitor the scheme. This should include annual reviews of the scheme's operation and working practices and, where appropriate, recommendations for improvements.

Where schemes operate within the public domain, an independent audit should be conducted before the publication of the annual report. This audit should include the following:

a) the level of attainment of objectives and procedures;
b) random audits of all logs and the release of information;
c) the review policy; and
d) standard costs for the release or viewing of material.

The complaints procedure should be reviewed, with the following details included:

1) the number of complaints received;
2) the time taken to acknowledge and respond to complaints;
3) the method of receiving and handling complaints; and
4) the degree of customer satisfaction in handling complaints.

NOTE 1 Further guidance on complaints management systems can be found in BS ISO 10002.

NOTE 2 Attention is drawn to Principle 10 of the Surveillance Camera Code of Practice [7].

4.4 Management and operation responsibilities

4.4.1 General

The owner of the scheme is accountable and should be clearly identified.

NOTE 1 Attention is drawn to the Data Protection Act 1998 [1] in relation to the data controller.

The owner may appoint a manager as their representative but should give the manager clear objectives and authority. These objectives should not be changed without the formal approval of the owner and they should be reviewed on a regular basis, at least annually.

There should be a clearly documented hierarchy of responsibility or delegated responsibility for all parties involved in the ownership, management, control and supervision of a CCTV scheme.

Responsibilities should be allocated for each individual; in the case of small CCTV systems, one person may be identified as being responsible for some, or all, of the requirements. It should be the responsibility of all parties connected with a CCTV scheme to maintain a continuous review of its integrity, security, procedural efficiency and methods of operation in respect of the gathering, retention and release of data. In addition, the policy should identify any individual(s) who have responsibility for the day-to-day management of a CCTV system.

NOTE 2 Attention is drawn to Principles 4 and 5 of the Surveillance Camera Code of Practice [7].

4.4.2 Owner

The identity and official address of the owner of a CCTV scheme should be clearly stated (e.g. website, signage). Where there are a number of partners in a scheme, one partner should be identified as the owner.

NOTE 1 The owner has the primary responsibility for ensuring compliance with the objectives of the policy and for ensuring effective management of it. This includes maintenance of the integrity and security of the CCTV scheme and the protection of the rights and interests of the public and individuals.

The owner is responsible for producing and implementing a written policy; this process should include consultation with users of the CCTV scheme and provision for the release of information relating to operation and carrying out a privacy impact assessment.

NOTE 2 The owner is responsible for amending or changing the policy in the light of operational experience or changes to the CCTV scheme.

The owner should ensure that complaints are addressed and that any subsequent requirement for change of procedures is dealt with. Where any of the management or supervisory responsibilities are delegated to a contractor, the owner should retain overall responsibility for the CCTV scheme and ensure formal monitoring of compliance with the contract in accordance with Annex C.

Where any management or operation of CCTV traffic enforcement cameras are used, the recommendations in Annex D should be adhered to.

The owner should comply with BS 7499 in the selection and recruitment of staff.

NOTE 3 Attention is drawn to Principles 1 and 9 of the Surveillance Camera Code of Practice [7] and Principle 2 of the Data Protection Act 1998 [1].

4.4.3 Manager

As the person with direct control of the CCTV scheme, the manager is responsible to the owner and should have authority for the following:

a) staff management (if appropriate);

b) observance of the policy and procedural practices;

c) release of data to third parties who have a legal right to copies;

d) control and security clearance of visitors;

e) security and storage of data;

f) security clearance of persons who request to view data;

g) release of new, and destruction of old, data and data media;

h) liaison with the law enforcement agencies and other agencies;

i) maintenance of the quality of the recording and monitoring equipment; and

j) responsibility for maintenance of discipline on a day-to-day basis.

The manager should retain responsibility for the implementation of procedures to ensure that the CCTV system operates according to the objectives for which it was installed and in accordance with the objectives identified for the CCTV scheme.

The manager is responsible for the day-to-day liaison with all partners in, and users of, the CCTV scheme; this should include supervision of access to any data obtained by the CCTV scheme.

The manager should have responsibility for the instigation of disciplinary procedures against operators in matters relating to non-compliance with this British Standard, operational procedures and breaches of confidentiality or the unauthorized release of data.

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

NOTE 2 Attention is drawn to the Data Protection Act 1998 [1] in relation to the data controller.

4.4.4 Supervisor

The supervisor should ensure that, at all times, the CCTV scheme is operated in accordance with its policy and all procedural instructions relating to the CCTV scheme, and should bring to the immediate attention of the manager any matter affecting the operation of the CCTV scheme, including any breach (or suspected breach) of the policy, procedural instructions, security of data or confidentiality.

The supervisor should ensure that, at all times, operators carry out their duties in an efficient and responsible manner, in accordance with the objectives of the CCTV scheme. This should include regular checks and audit trails to ensure that the documentation or computer records, in the case of digital systems, are working effectively.

Data recording systems should include:

a) still or print log;

b) the operator's log;

c) the incident log;

d) the maintenance log;

e) witness statements; and

f) authorized visitors.

The supervisor should ensure that operators carry out their duties in accordance with good practice and that they comply with the scheme's health and safety requirements.

NOTE 1 Attention is drawn to the Health and Safety at Work etc. Act 1974 [10] and the Working Time (Amendment) Regulations 2002 [11].

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

4.4.5 Operator

The operator should work under the direction of the owner, manager or supervisor and in accordance with the policy and procedural practices.

Operators should be proficient in the control of cameras and operation of all equipment forming part of the CCTV scheme. They should acquire a good knowledge of the area covered by the camera and ensure that information recorded or obtained by the CCTV scheme is accurate, adequate, relevant and does not exceed that which is necessary to fulfil its objectives. Operators should have been appropriately screened for handling personal data and images.

NOTE Attention is drawn to Principles 2, 6, 7, 8, 9 and 11 of the Surveillance Camera Code of Practice [7], Principles 1, 2, 3, 7 of the Data Protection Act 1998 [1] and the Private Security Industry Act 2001 [6].

The operator training and screening undertaken should be appropriate to the nature of surveillance camera system they are operating.

Operators should be responsible for the day-to-day operation of the CCTV scheme in accordance with the policy and procedural instructions. The integrity of a CCTV scheme depends very much upon the activities of operators, who should observe the civil rights of the public and individuals, and also respect their privacy.

Operators should be responsible for taking appropriate action to deal with incidents detected by the camera, in accordance with the procedures given in the policy, and should then record such information as required by procedural instructions in the appropriate log.

Operators should bring to the immediate attention of the supervisor any defect to equipment or picture transmission that adversely affects the operation of the CCTV system.

4.4.6 Contractor

Contractors should comply with Annex C, Annex D or Annex E, as applicable, which contain the elements of this British Standard that are applicable to contractors managing and operating CCTV schemes.

Special conditions should be drawn up for contractors who are engaged in work (e.g. installation, maintenance, operational, staffing) which comes within the scope of this British Standard.

NOTE Attention is drawn to Principles 7 and 8 of the Data Protection Act 1998 [1].

5 Personnel

*COMMENTARY ON CLAUSE **5***

Attention is drawn to the Private Security Industry Act 2001 [6].

5.1 Security screening

All personnel whose employment involves, or might involve, the acquisition of information, or access to information, images or equipment (the improper use of which could involve a risk to the security of the organization, any customer of the organization, or any third party) should be security screened in accordance with BS 7858.

NOTE This applies to all personnel, irrespective of whether they are engaged full-time or part-time, or on a permanent or temporary basis.

5.2 Recruitment and selection

Recruitment and selection should be carried out in accordance with BS 7499.

5.3 Training

New staff should be supervised until the training is complete. Training should be carried out by suitably qualified persons.

Training should include the following:

a) working conditions/terms of employment (including information about health and safety regulations);

b) the use of all appropriate equipment;

c) the operation of all appropriate systems (including knowledge of all sites to be monitored);

d) the management of recorded material, including the requirements for handling and storage of material needed for evidential objectives;

e) all relevant legal issues and codes of practice, e.g. the Surveillance Camera Code of Practice [7] and the Information Commissioner's *CCTV Code of practice* [8];

f) privacy and disclosure issues; and

g) the disciplinary policy.

The training plan should also provide the following:

1) the means to evaluate the effectiveness of the training given;

2) the delivery of further training where this is identified as being necessary;

3) a scheme of ongoing continuous development; and

4) the maintenance of records of all training given.

NOTE 1 BS 7499, BS 5979 and BS 8591 give further guidance on training.

The period of training should be sufficient to ensure that staff are able to carry out the specified duties.

Good training is essential to achieve effective and proper use of CCTV; the operator should be trained to be able to react to potential incidents, to monitor the event accurately and not lose information that could be pertinent to any future investigation.

NOTE 2 Attention is drawn to the Criminal Procedure and Investigation Act 1996 [12], which lists procedures that ensure all relevant information, including that which could substantiate the case for the defence, is catalogued.

6 CCTV control centre

6.1 General

A CCTV control centre should be a dedicated building, or a room within a building. The CCTV control centre should be kept locked, both while in use and if evacuated. Toilet and kitchen facilities for CCTV control centre staff should be provided.

The needs of lone workers in single staffed CCTV control centres should be taken into account.

NOTE 1 See BS 8484 for guidance on the provision of lone worker device services.

The CCTV control centre should have the means of communication with the emergency services, so that immediate contact can be made in times of emergency or during incidents.

Access to the CCTV control centre should be strictly controlled, including during changes of shift. All visitors and contractors entering and exiting the CCTV control centre should sign a visitors' log.

Where a CCTV control centre is not under law enforcement agency control, law enforcement agency officers should be granted the right to enter the CCTV control centre at any time for liaison and security objectives; this procedure should be agreed to and documented. Law enforcement agency officers should always sign the visitors' log.

NOTE In a centre which conforms to BS 5979 and BS 8591, adherence to the access protocols is required by law enforcement agencies.

6.2 Ergonomics

The CCTV control centre should be designed in accordance with good ergonomic practice. The following should be factored into the design:

a) architectural factors (including the design and layout of the room itself);

b) design and layout of individual work stations;

c) arrangement of monitors;

d) design of control panels;

e) seating; and

f) environmental factors (including heating, lighting and ventilation).

NOTE 1 BS EN ISO 11064-1, BS EN ISO 11064-2 and BS EN ISO 11064-3 give relevant information on ergonomic design.

NOTE 2 Attention is drawn to the Equality Act 2010 [13].

6.3 Health and safety

The shift patterns should be documented and sufficient breaks should be included to ensure the health and productivity of the operating staff.

NOTE 1 Attention is drawn to current health and safety legislation, about which all employees are informed under the induction training.

NOTE 2 Attention is drawn to the Health and Safety (Display Screen Equipment) Regulations 1992 [14], Regulation 4.

NOTE 3 Attention is drawn to the Working Time (Amendment) Regulations 2002 [11].

7 Incident handling

7.1 General

When an incident is captured by a CCTV system, the procedures detailed in **7.2** to **7.5** should be followed.

7.2 Incident policy

In the event of an incident (see **3.11**), action should be taken in accordance with local procedures.

A record of all incidents should be maintained by CCTV operators in the appropriate incident log. The information to be recorded should include anything of note that might be useful for investigative and evidential purposes or future system assessment and evaluation.

NOTE Attention is drawn to the obligations placed upon investigators by the Criminal Procedure and Investigation Act 1996 [12].

All recorded material and written records in connection with a CCTV scheme can be deemed to be material obtained in the course of a criminal investigation, which might be relevant to the investigation; therefore, all of this information should be disclosable to the defence in the event of a prosecution.

7.3 Incident response

The local procedures should identify who is responsible for making the response to an incident.

NOTE Depending on the incident, the response might be by emergency services, private security, roadside assistance, etc.

7.4 Timescale of the incident notification

The time at which the incident is notified to the responder(s) should be documented.

7.5 Incident observation and/or recording

The local procedures should indicate the times at which incident observation and/or recording is needed.

NOTE The local procedures might include the time immediately after an incident (direct incident response), for example:

a) until arrest/curtailment; or

b) during a whole incident, initiated by an alarm.

8 Privacy and disclosure issues

8.1 Privacy

Cameras should not be used to infringe an individual's rights to privacy. Ideally, privacy zones should be programmed into the CCTV system as required, in order to ensure that the interiors of any private properties within the range of the CCTV scheme are not viewed.

Operators should be made aware that misuse of the cameras (i.e. the use of cameras for objectives other than those for which they are intended) might constitute a breach of the law (see **4.4.5**).

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

8.2 Disclosure of data

8.2.1 General

The following principles should be included in the disclosure policy of the CCTV scheme.

a) Recorded material should only be used for the defined objectives in the policy (see **4.1** and **4.2**).

b) Access to recorded material should only take place in accordance with the policy and procedures.

c) There should be specific prohibitions on the disclosure of data for commercial purposes and entertainment purposes.

The policy should cover procedures for the release of personal data.

NOTE 1 Attention is drawn to the Data Protection Act 1998 [1].

NOTE 2 For guidance on information security, see BS ISO 27001.

8.2.2 Request to disclose data

*COMMENTARY ON **8.2.2***

A request to disclose data obtained from a CCTV scheme can be made by third parties for the purposes of:

a) providing evidence in criminal proceedings (attention is drawn, for example, to the Police and Criminal Evidence Act 1984 [15] and the Criminal Procedure and Investigation Act 1996 [12]);

b) providing evidence in civil proceedings;

c) the prevention and reduction of crime and disorder;

d) the investigation and detection of crime (including the identifying of offenders);

e) identifying witnesses; and

f) public interest.

Parties who are able to show adequate grounds for disclosure include the following:

1) law enforcement agencies;

2) statutory authorities with powers to prosecute;

3) solicitors; and

4) other agencies and persons (including the media), according to purpose and status.

The owner should not obstruct a bona fide third-party investigation to verify the existence of relevant data (see **4.3.3**).

The owner should not destroy data that are relevant to a previous or pending search request, which could become the subject of a subpoena.

NOTE 1 There might be occasion for a defence solicitor to make enquiries that fall outside the requirements of the disclosure legislation, for example investigating a client's alibi, notwithstanding evidence submitted to the Crown Prosecution Service (CPS), but the defence enquiry would have nothing to do with the prosecution investigation. Defence enquiries might also arise in a case where there was no recorded evidence in the prosecution investigation.

In the event that a defence solicitor makes enquiries for information that might fall outside the requirements of the disclosure legislation, the owner should ensure that the requested data have no connection with any existing data already passed to the law enforcement agencies. Furthermore, the owner should treat the defence enquiry confidentially.

NOTE 2 Disclosure does not necessarily include provision of a copy of the data so that this practice would fall within these guidelines.

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

8.3 Subject access disclosure (a named subject)

*COMMENTARY ON **8.3***

Attention is drawn to the provisions for subject access rights under the Data Protection Act 1998 [1]. If a request is made for personal data, it can be provided in two ways.

- *The data is viewed in a controlled environment.*
- *A copy of the personal data pertaining to that person is supplied.*

The owner/data controller should verify the validity of the request. Furthermore, the owner should treat the enquiry confidentially. Wherever possible, only personal data that are specific to the search request should be provided and the following should be taken into account.

a) If data are viewed, then obscuring other images on the data is unnecessary.

b) If a copy is required, then other individual personal data should be obscured.

Where there is no on-site means of obscuring other personal data, then the material should be sent to an editing house for processing prior to the personal data being provided to the individual. There should be a contractual agreement between the data controller and the editing house.

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

NOTE 2 A search request needs to contain sufficient information to locate the data requested (e.g. in 30 min slots for a given date and place). If inadequate or inaccurate information is provided, a data controller may refuse a request until sufficient information is provided.

8.4 Media disclosure

Set procedures for release of data to the media should be followed. If the means of obscuring other personal data does not exist on site, the data controller should ensure the following measures are adhered to.

a) The release document should take the form of a contract signed by both parties.

b) The material should be accompanied by a signed release document that clearly states what the data are to be used for and sets out the limits on their use.

c) The release document should state that the receiver has to process the data in a manner prescribed by the data controller, e.g. it should specify that identities/data should not be revealed.

d) The proof of editing should be passed back to the data controller, either for approval or final consent (protecting the position of the data controller, who would be responsible for any infringement of data protection legislation).

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

9 Recorded material management

9.1 General

The CCTV system should be capable of meeting the objectives of the CCTV scheme.

The CCTV system should be maintained in good working order and in accordance with the manufacturer's recommendations. Details of maintenance should be recorded from the date of purchase and be available for inspection.

Details of the recording and monitoring equipment used should be recorded.

Recorded material should be of the quality required by the courts if it is to be admitted in evidence; it is essential, therefore, that recorded material evidence maintains total integrity and continuity at all times.

Modern technology enables data to be recorded and stored on a variety of recording materials; the recommendations set out in this British Standard should be applied and modified to suit the specific recording material being used by a CCTV system.

NOTE 1 For electronic document management systems, see BIP 0008-1, BIP 0008-2 and BIP 0008-3.

Security measures should be taken to prevent unauthorized access to, or alteration, disclosure, destruction, accidental loss or destruction of recorded material.

A hard copy print should not be made as a matter of routine. When such a print is made, however, the person making the print should be responsible for recording the full circumstances under which the print is taken, with reasons, in accordance with procedures. Ideally, each print should be allocated a unique number, recorded in the appropriate log.

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

9.2 Media use, storage and disposal

Recorded material should be stored in a secure environment, so that the integrity of the media is maintained. This includes recorded material that has been requested by law enforcement agencies or contains a known incident. Controlled access to the recorded material storage area should be strictly maintained. Data that are to be destroyed should be destroyed under controlled operation.

Ideally, in analogue CCTV systems, new (unused) tapes should be used for recordings, although tapes may be reused in a controlled manner.

If tapes are reused, then there should be a written policy as to the maximum number of times that a tape is to be reused.

NOTE 1 No more than 12 times reuse is often recommended, because the quality of the recording degenerates considerably with each reuse.

Other important factors that reduce the life span of a tape and which should therefore be taken into account include:

a) replaying on a faulty machine;

b) jamming;

c) time lapse use;

d) frequent use of pause mode;

e) use in a dirty environment; and

f) not cleaning the tape heads regularly.

If tapes need to be reused, they should first be erased by a bulk erasure machine and the action recorded.

NOTE 2 Degaussing of tapes is an acceptable means of erasing tapes.

To control the number of times a tape is reused, the use of each videotape should be recorded, for example by attaching a spine label to the cassette tape and the cassette tape box. Each time the tape is used, the label on the cassette and the box should be initialled by the operator, so that the number of uses are readily identified.

Once purchased, the life of any videotape should be fully documented (see **9.3**).

9.3 Recorded material register

A CCTV system should have a register showing the life of the media at all stages whilst in the owner's possession; such a register might also show itself to be useful in enabling evaluation of the CCTV scheme.

Before use, the media should be indelibly marked, ideally on the body, with a unique reference number.

The register should include the following information:

a) unique media reference number(s);

b) details of purchase (i.e. from whom purchased and delivery date);

c) time/date/person placing the media in store;

d) time/date/person removing the media from secure storage for use;

e) time/date/person returning the media to secure storage after use;

f) remarks column to cover additional points (e.g. erased/destroyed/handed over to law enforcement agencies/removed from recording machine);

g) time and date of delivery to the law enforcement agencies, identifying the law enforcement agency officer concerned;

h) in the event of a non-automated system of erasure of data, the time/date/person responsible for erasure and/or destruction; and

i) for videotape, the tape type and batch number.

NOTE The register might be a bound book with printed, numbered pages to prevent loose-leaf pages being removed and/or replaced. Alternatively, the register might be electronic.

9.4 Making recordings

When making recordings the following procedure should be followed.

a) Before recording, test that all equipment is working correctly.

b) When using an analogue CCTV system, ensure the tape counter on the video recorder(s) is set at zero.

c) Check time/date generator is correctly displayed.

d) When using an analogue CCTV system, record time and date of loading, and the tape identification. Any additional information should be included in the tape register.

e) Maintain records of the operator(s) of the equipment. This enables the manager to establish who was operating the equipment at any given time.

f) Record without interruption, wherever practicable. Any interruption should be logged.

g) When using an analogue CCTV system, on completion of the recording, remove the tape from the recorder.

Media containing original incidents should not be replayed, unless essential; this is to avoid any accident, damage, manipulation or erasure. If a medium needs to be reviewed, the reasons should be logged, together with the time of review, media identity and identity of persons reviewing the media. When using analogue CCTV systems, tapes should be returned, after use, to secure storage, and recorded in the videotape register.

All documentation should be auditable.

NOTE When using digital CCTV systems, see the processes outlining the export of media in Digital imaging procedure *[16] and* UK police requirements for digital CCTV systems *[17].*

9.5 Tape loading/unloading for analogue CCTV systems

If appropriate, a set time should be established for tapes to be loaded and unloaded from the machine, regardless of the length of time that they have been running, at the most operationally convenient time (for example, when there is the least likelihood of incidents).

When a tape is released for evidential purposes, a replacement tape should be inserted immediately and noted accordingly in the appropriate register. The next tape should be inserted at the agreed set time.

All documentation should be completed at the time of the task being carried out and not retrospectively.

10 Documentation

10.1 General

It is essential that accurate and full records be maintained; logbooks or databases should be sequential so that pages or entries cannot be removed or overwritten.

NOTE 1 Computer programs may be used for this purpose provided nobody can tamper with, or edit, them after the event.

NOTE 2 If records are maintained on an electronic document management system, see BIP 0008-1, BIP 0008-2 and BIP 0008-3 for guidance.

10.2 Logs

An accurate log should be maintained of which operators were working at a given time/date and, if appropriate, the camera(s) they were controlling.

NOTE These logs can be maintained within a computerized system.

An operator's log should be available at each workstation and should be completed at the time of operation by the operator in question. The details of any event or occurrence that might be required for future reference should be recorded; these include the following:

a) change of operator, identifying the operator on duty at that workstation and showing that the necessary recording material has been loaded in the correct recording equipment, that the correct time was being displayed and that the recording equipment appeared to be operating correctly;

b) incidents, including details of the time, date, location, nature, operator and action taken;

c) routine camera patrols, whether undertaken manually or through the utilization of pre-set times; and

d) privacy zones, detailing where, for any reason, it is necessary to encroach on private areas that are not part of the patrol (see **8.1**).

10.3 Administrative documents

*COMMENTARY ON **10.3***

Administrative documents covers any records considered necessary to facilitate the efficient running of the scheme and varies according to the objective of the scheme.

The following administrative documents should be maintained:

a) recorded material register (see **9.3**);

b) recorded material management (register of the management of recording incoming/outgoing telephone calls and radio traffic) (see Clause **9**);

c) log of daily routine administrative events, including details of the following:

   1) visitors to the control room;

   2) demonstrations of the CCTV surveillance operation to outside bodies, groups, etc.;

   3) maintenance of equipment, whether routine or breakdown repair;

   4) administrative activities within the control room;

   5) staff signing on and off duty; and

   6) any out of the ordinary activity or occurrence;

d) shift register, containing duty, weekly leave and annual leave details of all staff; and

e) list of all installed equipment.

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

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

The *Surveillance Camera Code of Practice* [7] gives the good practice principles that any end user ought to take into account before acquiring, when using and when auditing a CCTV surveillance system.

Table A.1 gives the 12 guiding principles of the *Surveillance Camera Code of Practice* [7] and shows where they are called up in the main text of this British Standard.

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

Number	Principle from the *Surveillance Camera Code of Practice* [7]	Clause in BS 7958
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.	**4.1.1, 4.4.2**
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.	**4.2.2, 4.4.5, 8.1**
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.	**4.1.3**
4	There must be clear responsibility and accountability for all surveillance camera system activities, including images and information collected, held and used.	**4.3.1, 4.4.1, 4.4.4**
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.	**4.2.1, 4.3.1, 4.4.1**
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.	**4.3.2, 4.4.5, 9.1**
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.	**4.3.3, 4.3.4, 4.4.4, 4.4.5, 8.2.2, 8.3, 8.4, 10.3**
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.	**4.4.5**
9	Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.	**4.3.2, 4.4.2, 4.4.5**
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.	**4.3.6, 4.3.7**
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.	**4.1.2, 4.2.2, 4.4.5**
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.	**4.3.4**

Annex B (informative)

Data Protection Act 1998 – 8 guiding principles

The Information Commissioners Office has published a document, *In the picture: A data protection code of practice for surveillance cameras and personal information* [18]. This sets out best practice for data protection issues using CCTV systems.

Table B.1 gives the 8 guiding principles of the Data Protection Act 1998 [1] and shows where they are called up in the main text of this British Standard.

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

Number	Principle	Clause in BS 7958
1	Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless – a) at least one of the conditions in Schedule 2 is met, and b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.	**4.4.5**
2	Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.	**4.1.1**, **4.4.2**, **4.4.5,**
3	Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	**4.1.2**, **4.4.5**
4	Personal data shall be accurate and, where necessary, kept up to date	**4.1.2**, **4.2.2**, **4.3.4**, **4.4.3**, **4.4.4**
5	Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.	**4.2.1**, **4.2.2**, **4.3.4**, **4.4.3**, **9.1**
6	Personal data shall be processed in accordance with the rights of data subjects under this Act.	**4.1.3**, **4.3.1**, **8.1**, **8.2.2**, **8.3**, **8.4**, **10.3**
7	Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	**4.3.1**, **4.4.3**, **4.4.4**, **4.4.5**, **4.4.6**
8	Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	**4.4.6**

Annex C (normative) Contractor responsibilities within BS 7958

COMMENTARY ON ANNEX ***C***

This annex gives recommendations for the management and operation of CCTV schemes for contractors providing personnel to the owner's CCTV control centre, operating such schemes on behalf of the owner, in areas where the public are encouraged to enter or have a right to visit. It also applies to commercial CCTV schemes covering areas where the public do not have the same rights of access that are either operated by the owner of the area (property) or on their behalf.

Closed circuit television (CCTV) schemes that process data about a known person 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] and the Protection of Freedom Act 2012 [4]. This code of practice is designed to supplement that legislation and aims to ensure fairness, objectivity and responsibility.

Attention is 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.

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

C.1 General

When applying the recommendations of this British Standard, a contractor should adhere to the following underlying objectives.

a) For CCTV control centres who offer other types of contracted monitoring services with the aim of gaining an emergency response, the control centre should meet the recommendations of BS 5979 or BS 8591.

   NOTE Refer to the NPCC policy on police requirements and response to security systems *[19].*

b) The reliability of the monitoring service should be ensured by the provision of an adequate number of competent personnel supported by the necessary domestic facilities.

c) The monitoring service should be resilient to disruption by foreseeable events that may affect the remote centre or the transmission network.

C.2 Principles and management of the CCTV scheme

C.2.1 Management responsibilities

C.2.1.1 Manager

The recommendations of **4.4.3** should be followed.

C.2.1.2 Supervisor

The recommendations of **4.4.4** should be followed.

C.2.1.3 Operator

The recommendations of **4.4.5** should be followed.

C.2.2 Personnel

The recommendations of Clause **5** should be followed.

C.2.3 CCTV control centre

C.2.3.1 General

The recommendations of **6.1** should be followed.

C.2.3.2 Health and safety

The recommendations of **6.3** should be followed.

C.2.4 Response

C.2.4.1 Incident policy

In the event of an incident being observed by a CCTV operator, action should be taken in accordance with local procedures.

A record of all incidents should be maintained by CCTV operators in the appropriate incident log. The information to be recorded should include anything of note that might be useful for investigative and evidential purposes or future system assessment and evaluation.

NOTE Attention is drawn to the obligations placed upon investigators by the Criminal Procedure and Investigation Act 1996 [12].

Any matter for scheme management should also be recorded and relayed to the appropriate supervisor/manager for appropriate follow-up action.

C.2.4.2 Time scale of the response

The time at which the incident is notified to the relevant authority should be documented.

C.2.4.3 When observation and/or recording is needed

The recommendations of **7.5** should be followed.

C.2.5 Privacy and disclosure issues

Managers should ensure that the recommendations of Clause **8** are followed whenever they are carried out by the contracted personnel.

Operators should be made aware that misuse of the cameras (i.e. the use of cameras for objectives other than those for which they are intended) might constitute a breach of the law.

NOTE Attention is drawn to the Data Protection Act 1998 [1] and the Protection of Freedoms Act 2012 [4].

C.2.6 Recorded material register

C.2.6.1 Media use, storage and disposal

The recommendations of **9.2** should be followed.

C.2.6.2 Making recordings

The recommendations of **9.4** should be followed.

C.2.6.3 Tape loading/unloading for analogue CCTV systems

The recommendations of **9.5** should be followed.

C.2.7 Documentation

C.2.7.1 Logs

The recommendations of **10.2** should be followed.

C.2.7.2 Administrative documents

The recommendations of **10.3** should be followed.

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

*COMMENTARY ON ANNEX **D***

This annex gives recommendations for the management and operation of CCTV traffic enforcement cameras. This is to ensure operators are aware of the correct procedures in the case of an incident. Its recommendations facilitate the detection of offenders in relation to non-compliance with existing traffic regulations, as a measure to improve the reliability and punctuality of public transport and also to satisfy the community over the competence of the system and its operators.

This annex can be used to complement the monitoring station's own code of practice and gives recommendations for the operation and management of CCTV within a controlled environment, where data that might be offered as evidence are received, stored, reviewed or analysed.

Attention is drawn to the Traffic Management Act 2004 [20], the Protection of Freedoms Act 2012 [4] and the Data Protection Act 1998 [1].

D.1 Principles and management of the CCTV scheme

D.1.1 Procedures

For the purpose of this annex, procedures should be carried out in accordance with **4.3**.

D.1.2 Audit

For the purpose of this annex, the audit should be carried out in accordance with **4.3.7**.

D.1.3 Annual report

For the purpose of this annex, the annual report should be prepared in accordance with **4.3.6**.

D.1.4 Management responsibilities

D.1.4.1 General

All personnel involved in the acquisition of data should be security screened in accordance with BS 7858.

D.1.4.2 Owner

For the purpose of this annex, the owner's responsibilities should be carried out in accordance with **4.4.2**.

D.1.4.3 Manager

For the purpose of this annex, the manager's responsibilities should be carried out in accordance with **4.4.3**.

D.1.4.4 Supervisor

For the purpose of this annex, the supervisor's responsibilities should be carried out in accordance with **4.4.4**.

D.1.4.5 Operator

For the purpose of this annex, the operator's responsibilities should be carried out in accordance with **4.4.5**.

D.2 Recording equipment

D.2.1 General

There should be dual recordings, one being nominated the master copy and the other a working copy.

NOTE The purpose of dual recording is that the master is the monitoring station copy and the slave a working copy.

The medium for recording should be by videotape or digital and should be able to record at a minimum rate of five frames/images per second. Each frame/image should be timed (hours, minutes and seconds), dated and sequentially numbered automatically.

D.2.2 Recorded images

All cameras should be capable of providing a close-up image of the vehicle number plate to enable number plate recognition as well as a wide-angle image to provide information about any mitigating circumstances surrounding the alleged contravention, which might be used in an appeal.

D.2.3 Printed image

Any printed image should contain the exact time and date when the frame was captured as well as its unique reference number.

D.2.4 Voice-over

Recordings made with voice-over should be timed stamped, dated and sequentially numbered.

D.2.5 Degaussing equipment

Where appropriate, the monitoring station should be equipped with degaussing equipment, which should be used on all videotapes before reuse and disposal. Only clean tape should be used.

D.3 Monitoring of traffic

D.3.1 General

Camera enforcement signs should be displayed in areas where the system operates.

Cameras should be connected to a monitoring station by an encrypted data link. The matrix or recording equipment should be synchronized to a time standard using an atomic clock, or to a signal from recognized similar independent output.

D.3.2 Operator's duties

D.3.2.1 Logging on

Only trained and qualified operators should use the system (see **5.3** and **D.7.2**). The first duty of an operator should be to fill out the log sheet (see the example in Figure D.1) and then follow the set out procedures in Clause **9** and/or the customer's/operator's guide/code of practice.

D.3.2.2 Recorded media

The procedure for dealing with the recording material should be clearly defined within the operator's guide.

D.3.2.3 Monitoring of traffic

The operator should operate cameras in such a way as to avoid unwarranted invasion of privacy and to prevent them from being used for any purpose other than traffic enforcement or non-traffic incidents (see **D.3.2.5**).

D.3.2.4 Contravention of traffic regulations

When a traffic contravention is identified while operating the camera in real time, the operator should obtain the most effective images of the vehicle and its surrounding circumstances. Contraventions should be identified at the time they are committed, and not at some subsequent time from pre-recorded tapes or digital recordings. When evidence of the contravention has been recorded the operator should record the time in hours and minutes. The operator should record the vehicle's details, i.e. registration plate, make, model, colour, etc. in the occurrence log (see Figure D.2) or by using approved audio equipment.

NOTE Attention drawn to the Traffic Management Act 2004 [20].

D.3.2.5 Non-traffic incident

When a non-traffic incident is recorded, the operator should adopt procedures agreed locally with the police and other scheme partners in accordance with this British Standard. All such incidents should be recorded on the log sheet (for an example see Figure D.1).

NOTE The log sheet can also be used to record equipment faults.

D.3.2.6 Traffic contravention

When a traffic contravention is observed, the operator should ensure all possible mitigating circumstances are checked and the details recorded in the occurrence log (for an example see Figure D.2).

D.3.2.7 End of monitoring period

At the end of the monitoring period, or as otherwise dictated by local procedures, the operator should:

a) log the exact time (in hours and minutes) and final incremental number from the recorder;

b) remove the evidence copy;

c) seal the master media in an evidence bag, retain working copy to review, having allocated it a unique reference number; and

d) put the master copy in secure storage.

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

Date	Operator's name	Start time	Finish time	Camera no./ID	Tape no.	Comments/equipment fault
Name of supervisor:..... Signature:.....						

Figure D.2 **Example of occurrence log**

Date	Start time	End time	Tape no./ID	Camera no./ID	Vehicle registration	Make	Model	Colour	Location	PCN no.
Operator's name: ..... (Print) Number:.....										

D.4 Management of evidence

D.4.1 Operator evidence

All records made during a monitoring period should be retained in secure storage.

NOTE 1 Observation of a contravention by the operator is the direct evidence.

NOTE 2 Attention is drawn to the Data Protection Act 1998 [1].

D.4.2 Video evidence

All monitoring and observations should be concurrently recorded on at least two devices, either videotape or digital medium. On both recordings, every frame/image should be timed and dated and stamped with a unique reference number.

NOTE One recording is the master recording (which is to be known as the evidence copy); the second recording is the slave (and is to be known as the working copy).

D.4.3 Evidence copy of recording media (master)

D.4.3.1 Storage

After each monitoring period the tape/digital evidence should be immediately removed/digitally transferred, sealed in an evidence bag and placed in secure storage. An accurate log should be maintained in accordance with **D.7.2**. The evidence should be retained until it is required for adjudication evidence, or is no longer required for this purpose.

D.4.3.2 Audit trail

All movement of evidence should be recorded, from its inception to when it is erased or destroyed. Destruction of the tapes/digital medium should be carried out by a contractor in accordance with BS EN 15713 and a log should be maintained.

D.4.3.3 Reuse of master

The master should only be re-used when all contraventions recorded on it have been fully processed in accordance with the monitoring station procedure.

D.5 Working copy

D.5.1 Reviewing and storage

The working copy should be reviewed at the end of each monitoring period for potential contraventions.

Once a potential contravention is discovered the working copy should be retained in secure storage when not being processed. The working copy should only be removed from secure storage:

a) when called on to generate still images or photographs;

b) for release to third parties in accordance with **D.5.4**; or

c) for the purpose of additional monitoring.

D.5.2 PCN issue

The authorized representative should determine the issue of the PCN (penalty charge notice).

D.5.3 Appeals

Where relevant, and in line with the monitoring station's code of practice, the following items should be supplied to the adjudicators to assess a case that has been appealed.

a) A witness statement produced by the operator, stating the time the contravention was observed. Also, a detailed list of the evidence being presented and a copy of the CCTV monitoring station log sheet to determine the status of the equipment used to record the contravention.

b) A copy of the penalty charge notice.

c) A copy of the enforcement notice.

d) A copy of the notice of rejection.

e) A case summary which should include the relevant part of the regulation allegedly being contravened.

f) Photographic evidence.

g) Certificate of service (if required). When the certificate of service is required, it should be submitted to the adjudicator not less than seven days before the hearing confirming that copies of the above have been sent to the registered licence holder.

NOTE Attention is drawn to the relevant requirements of the Human Rights Act 1998 [2].

D.5.4 Release of recordings to third parties

All recordings are the property of the monitoring station and should not be copied or released from the monitoring station without formal authorization as defined in the monitoring station's code of practice. The working recording relevant to a particular contravention should only be released to the following individuals (or under the following circumstances):

a) traffic adjudicators;

b) police;

c) lawyers acting for appellants in traffic appeals;

d) lawyers acting for defendants; or

e) by court order, in connection with civil proceedings.

All images should have an audit trail to ensure the recorded material maintains total integrity and continuity at all times and to enable any images to be used for evidential purposes. If the recorded data are held on an electronic document management system, the system should conform to all parts of BIP 0008.

D.5.5 Reuse of working copy

The working medium should only be reused when all contraventions recorded on it have been fully processed.

D.6 Operating personnel selection and training

D.6.1 Selection

All individuals applying for relevant employment as operators for the monitoring of traffic offences should be security screened in accordance with BS 7858. The prospective employee should be asked to demonstrate that they have the physical ability, mental aptitude and intelligence to undertake the role of an operator. The employee should also be examined for literacy, sight, colour blindness and hearing.

D.6.2 Training

All employees should be trained in their responsibilities and roles in operating CCTV. When a potential incident occurs, the operator should be able to react to monitor the event accurately and not lose information that might be pertinent to any future investigation.

All personnel should receive training on health and safety in the workplace, first aid, and fire prevention and safety. Other training requirements should include:

a) terms of responsibility;

b) all use of appropriate equipment and operation of systems;

c) basic knowledge of traffic law;

d) the enforcement process;

e) knowledge of the areas to be monitored;

f) management of recorded material, including the requirements for handling and storage of material needed for evidential purposes;

g) disciplinary policy; and

h) attention to monitoring station equipment.

Operators should only be permitted to carry out the specified duties when they have successfully completed the relevant training.

D.7 Documentation

D.7.1 General

Accurate and detailed records should be maintained. A logbook or database should maintain a sequential order so pages or entries cannot be removed or overwritten.

NOTE A computer database can be used for this purpose as long as it cannot be compromised.

If records are maintained in a database then the system should conform to all parts of BIP 0008.

D.7.2 Logs

An accurate log should be maintained, recording which operators were working at any given time or date and which cameras they were controlling. Each workstation should have its own log, recorded by the operator, of the time and date of any event or occurrence that might be required for further evidence. The log should also record any changes of operator, malfunctions of the equipment or encroachments onto private areas that are not part of the contract.

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

*COMMENTARY ON ANNEX **E***

This annex gives recommendations for the management and operation of CCTV schemes for contracted remote CCTV control centres providing CCTV control centre facilities and monitoring services, operating such schemes on behalf of the owner, in areas where the public are encouraged to enter or have a right to visit. It also applies to commercial CCTV schemes covering areas where the public do not have the same rights of access that are either operated by the owner of the area (property) or on their behalf.

Attention is 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.

Closed circuit television (CCTV) schemes that process data about a known person are obliged to conform to certain legislation, most importantly the Data Protection Act 1998 (DPA) [1], the Human Rights Act 1998 (HRA) [2], the Protection of Freedom Act 2012 [4] and the Freedom of Information Act 2000 [3]. This code of practice is designed to supplement that legislation and aims to ensure fairness, objectivity and responsibility.

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

E.1 General

When applying the recommendations of this British Standard, a contracted remote CCTV control centre monitoring public space should adhere to the following underlying objectives:

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

a) The requirements for contacting and supplying data to the police in the area where the public space CCTV is being monitored should be defined in the contract.

b) For contracted remote CCTV control centres who offer other contracted monitoring services with the aim of gaining an emergency response, the control centre should meet the recommendations of BS 5979 or BS 8591.

NOTE 2 Refer to the NPCC policy on police requirements and response to security systems *[19].*

E.2 Principles and management of the CCTV scheme

E.2.1 Objectives

The recommendations of **4.1** should be followed as stated in the contract.

E.2.2 Policy

The recommendations of **4.2** should be followed as stated in the contract.

E.2.3 Procedures

E.2.3.1 Information security

The recommendations of **4.3.1** should be followed in so far as they apply to the contracted remote CCTV control centre.

The recommendations of **4.3.2** should be followed.

E.2.3.2 Access to data

The recommendations of **4.3.3** should be followed.

E.2.3.3 Supporting data

The recommendations of **4.3.4** should be followed.

E.2.3.4 Annual report

The contracted remote CCTV control centre should provide the scheme owner with information necessary to enable the scheme owner to provide an annual report in accordance with **4.3.6**. This information supplied should be set out in the contract.

E.2.3.5 Audit

The contracted remote CCTV control centre should provide information to the owner as necessary in accordance with **4.3.7** as it applies to the contracted service (i.e. it is not an independent audit of the contracted remote CCTV control centre, but an audit of the monitoring part of the owners CCTV system).

NOTE Attention is drawn to Principle 10 of the Surveillance Camera Code of Practice [7] and Principle 2 of the Data Protection Act 1998 [1].

E.2.4 Management responsibilities

E.2.4.1 General

The recommendations of **4.4.1** should be followed as stated in the contract.

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

E.2.4.2 Manager

The recommendations of **4.4.3** should be followed, in so far as they are applicable to the contracted remote services.

E.2.4.3 Supervisor

The recommendations of **4.4.4** should be followed.

E.2.4.4 Operator

The recommendations of **4.4.5** should be followed.

E.2.5 Personnel

The recommendations of Clause **5** should be followed.

E.2.6 CCTV Control Centre

The recommendations of Clause **6** should be followed.

E.2.7 Response

The recommendations of Clause **7** should be followed.

E.2.8 Privacy and disclosure issues

The recommendations of Clause **8** should be followed and the requirements of data disclosure should be detailed in the contact with the owner.

E.2.9 Recorded material management

The recommendations of Clause **9** should be followed.

E.2.10 Documentation

The recommendations of Clause **10** should be followed.

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS EN ISO 11064-1, *Ergonomic design of control centres – Part 1: Principles for the design of control centres*

BS EN ISO 11064-2, *Ergonomic design of control centres – Part 2: Principles for the arrangement of control suites*

BS EN ISO 11064-3, *Ergonomic design of control centres – Part 3: Control room layout*

BS ISO 10002, *Quality management – Customer satisfaction – Guidelines for complaints handling in organizations*

BS ISO 27001, *Information technology – Security techniques – Information security management systems – Requirements*

Other publications

[1] GREAT BRITAIN. Data Protection Act 1998 (DPA). London: The Stationery Office.

[2] GREAT BRITAIN. Human Rights Act 1998 (HRA). London: The Stationery Office.

[3] GREAT BRITAIN. Freedom of Information Act 2000. London: The Stationery Office.

[4] GREAT BRITAIN. Protection of Freedoms Act 2012. London: The Stationery Office.

[5] GREAT BRITAIN. Regulation of Investigatory Powers Act 2000. London: The Stationery Office.

[6] GREAT BRITAIN. Private Security Industry Act 2001. London: The Stationery Office.

[7] GREAT BRITAIN. Surveillance Camera Code of Practice. London: The Stationery Office, 2013. [1)]

[8] INFORMATION COMMISSIONER'S OFFICE. *CCTV Code of practice – Revised Edition*. Wilmslow: Information Commissioner, 2014.

[9] INFORMATION COMMISSIONER'S OFFICE. *Conducting privacy impact assessments code of practice*. Wilmslow: Information Commissioner, 2014.

[10] GREAT BRITAIN. Health and Safety at Work etc. Act 1974. London: The Stationery Office.

[11] GREAT BRITAIN. Working Time (Amendment) Regulations 2002. London: The Stationery Office.

[12] GREAT BRITAIN. Criminal Procedure and Investigation Act 1996. London: The Stationery Office.

[13] GREAT BRITAIN. Equality Act 2010. London: The Stationery Office.

[14] GREAT BRITAIN. Health and Safety (Display Screen Equipment) Regulations 1992. London: The Stationery Office.

[1)] Available from <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf> [last viewed 24 August 2015].

[15] GREAT BRITAIN. Police and Criminal Evidence Act 1984. London: The Stationery Office.

[16] POLICE SCIENTIFIC DEVELOPMENT BRANCH. *Digital imaging procedure – Version 1.0*. London: Home Office, 2002. [2)]

[17] CENTRE FOR APPLIED SCIENCE AND TECHNOLOGY, *UK police requirements for digital CCTV systems*, London: Home Office, 2005. [3)]

[18] INFORMATION COMMISSIONER'S OFFICE. *In the picture: A data protection code of practice for surveillance cameras and personal information.* Wilmslow: Information Commissioner, 2015.

[19] NATIONAL POLICE CHIEFS' COUNCIL (NPCC) of England, Wales and Northern Ireland. *NPCC policy on police requirements and response to security systems.* London: NPCC, June 2015.

[20] GREAT BRITAIN. Traffic Management Act 2004. London: The Stationery Office.

[2)] Available from <http://scienceandresearch.homeoffice.gov.uk/hosdb/> [last viewed 24 August 2015].

[3)] Available from <http://scienceandresearch.homeoffice.gov.uk/hosdb/> [last viewed 24 August 2015].

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™