National Security Inspectorate
Sentinel House, 5 Reform Road, Maidenhead, SL6 8BY
E: nsi@nsi.org.uk | W: nsi.org.uk

Dated: 17 August 2016

To:
1. All NSI Guarding Gold and Silver Companies who are approved for Closed Circuit Television (CCTV) Management and Operation
2. Applicant Companies who wish to gain approval for the above scope of approval

TECHNICAL BULLETIN No: 0032

Guidance on the implementation of BS 7958:2015, the British Standard Code of Practice for Management and Operation of Closed Circuit Television (CCTV)

(Supersedes BS 7958:2009)

BS 7958:2015 shows a publication date of the 31st August 2015 and is available through licensed outlets including NSI who can supply copies at a discounted rate.

BS 7958:2015 identifies requirements for the management and operation of CCTV schemes. Organisations that demonstrate compliance with BS 7958:2015, and also satisfy the relevant NSI criteria for approval, will be approved for the following scope:

"Closed Circuit Television (CCTV) Management and Operation".

The 2015 edition will now be applied to all NSI approval schemes where the criteria for approval require compliance with BS 7958 as a condition of NSI approval. The Standard will be applied with immediate effect, subject to the additional clarifications and guidance contained within this Technical Bulletin.

NSI also offers approvals against Annex C, Annex D and Annex E of BS 7958:2015. See Annexes for further information.

Implementation timescale for Applicant Companies

Applicant Companies will be audited against the 2015 edition with immediate effect and any Improvement Needs recorded against clauses of the Standard will have to be satisfactorily addressed before approval can be granted.

Implementation timescale for existing Approved Companies

Companies holding NSI approval to BS 7958:2009 will be expected to upgrade to BS 7958:2015 by the end of June 2017.

NOTE REGARDING THE STATUS OF BS 7958:2015

Although issued as a code of practice by the British Standards Institution, it is important to note that compliance with the recommendations given in BS 7958:2015 is regarded as mandatory for all companies wishing to maintain an NSI approval with respect to the provision of CCTV services; subject to any additional clarifications and guidance included within this Technical Bulletin or issued subsequently.

The recommendations given in BS 7958:2015 must therefore be regarded as requirements in relation to NSI approval for Closed Circuit Television (CCTV) Management and Operation.

DETAILS OF THE CHANGES
(Highlighted under the clauses of the new Standard)

Comments under each clause of BS 7958:2015 detail the changes when compared with the corresponding clause within BS 7958:2009.

Where the actual wording of the standard is quoted it is reproduced in bold text.

Where it is considered relevant to further clarify the specified requirement, additional guidance is included in italics.

We will consider alternative methods of achieving compliance with specified requirements where these can be demonstrated to be equivalent.

CONTENTS

The contents page of BS 7958 shows that the ten numbered sections have been retained.

The heading for section 6 reflects a change of terminology from 'CCTV Image Receiving Centre' to **CCTV control centre** and the heading for section 7 reflects a change of terminology from 'Response' to **Incident handling**.

New annexes have been added and numbering of annexes have been changed as follows:

Where previously **Annex A** (normative) of BS 7958:2009 related to Contractor responsibilities within BS 7958; Annex A (informative) of BS 7958:2015 now covers Surveillance Camera Code of Practice – 12 guiding principles.

Where previously **Annex B** (normative) of BS 7958:2009 related to Management and operation of CCTV traffic enforcement cameras, Annex B (informative) of BS 7958:2015 now covers Data Protection Act 1998 – 8 guiding principles.

Annex C (normative) of BS 7958:2015 now covers Contractor responsibilities within BS 7958.

Annex D (normative) of BS 7958:2015 now covers Management and operation of CCTV traffic enforcement cameras.

Annex E (normative) of BS 7958:2015 is a new annex covering Contracted remote CCTV control centre responsibilities within BS 7958. These responsibilities were understood to lie within Annex A of the previous standard whereas they are now clarified in the new Annex E.

Annexes C, D and E are normative which makes them a formal part of the standard (where applicable to the services provided).

The new List of tables consists of two tables: Table A.1 – 12 guiding principles of the Surveillance Camera Code of Practice and Table B.1 – 8 guiding principles of the Data Protection Act 1998.

FOREWORD

BS 7958:2015 was prepared by BSI Technical Committee GW/3 (Manned security services).

The Foreword clarifies that the 2015 edition **is a full revision of the Standard, which has been updated to reflect current good practice, and that it supersedes BS 7958:2009, which is withdrawn**.

INTRODUCTION

The introduction includes references to the Protection of Freedoms Act 2012 [4] and the Regulation of Investigatory Powers Act 2000 [5].

A statement has now been included that **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.

It is relevant to remind companies that it is a condition of any NSI approval that organisations comply with appropriate legislation and in particular if relevant individuals are not in possession of either the

appropriate SIA front-line or non-front-line licences then unless appropriate dispensations have been granted, NSI approval cannot be recommended or maintained.

The list of areas where CCTV schemes are used and the public would have a 'right to visit' include two new areas i.e. **e) sports grounds where access is unrestricted and f) public arenas such as sports stadiums and public places where events are held as an alternative to regular activities in those locations**.

The following two paragraphs of text have been deleted from the Introduction and incorporated in other relevant places within the new standard:

"This British Standard aims to provide recommendations on best practice to assist users in obtaining reliable information that can be used as evidence. Whilst some schemes might not need to meet the DPA [1] criteria, compliance with the code of practice is strongly recommended, particularly where schemes include an element of observation of the public.

"The clauses on the processing of data within this British Standard are applicable to the storage of recorded images/data from CCTV systems designed to operate normally in observation mode, e.g. garages, small shops, private businesses and private transport."

1 SCOPE

The clarification of the scope is the inclusion of a sentence under the first paragraph to show that the **standard now also applies to the monitoring of and management of public spaces, including automatic number plate recognition (ANPR) and traffic enforcement cameras**.

The second paragraph now includes the reference to **BS 8591** as well as BS 5979.

The scope has now been changed to cover also **traffic enforcement schemes**.

The scope now includes that **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).**

References to the Principles of the Surveillance Camera Code of Practice and the Principles of the Data Protection Act are given throughout the standard.

2 NORMATIVE REFERENCES

BS 8591 the code of practice for remote centres receiving signals from alarm systems has been added to the list of reference documents.

3 TERMS AND DEFINITIONS

A number of changes have been made in this area. The previous list of 36 definitions has been decreased to 30 by removing definitions not needed. Therefore the reference numbers for some definitions have changed. The new headings and any changes are listed below.

3.1 New title and definition for **CCTV control centre (previously CCTV Image Receiving Centre)**

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

The 2009 edition of BS 7958 only included a definition for a "central location for a CCTV scheme, where live images are monitored in real time and which has processing facilities".

3.2 CCTV scheme

There are no changes except the Note has been moved to 3.3.

3.3 CCTV system

There are no changes except the Note has been added from 3.2.

3.4 clean tape

No change.

3.5 Definition for **contractor** has been simplified:

party contracted by the owner to undertake agreed services

3.6 controlled environment

The definition of controller (see 3.6 in the 2009 edition) has been deleted and replaced with staff (see 3.27 in the 2015 edition). Consequently there are changes to the numbering of definitions.

The definition for **controlled environment** has now been replaced with:

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

No change.

3.8 data

No change.

3.9 evidence copy

The title of the definition has changed from **evidential copy** to **evidence copy** and the word 'second' has been removed from the definition, which is as follows:

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

3.10 hard print copy

No change.

3.11 Definition for **incident** has been simplified:

activity that warrants a response

3.12 New definition for **local procedures**:

documents relating to the processing of aspects of the CCTV scheme

3.13 Slight change to title of definition for **manager(s)** as there might be more than one manager.

3.14 Revised definition for **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 Slight change to the definition for **monitoring period** as there might be more than one procedure.

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

3.16 operator

No change (was 3.18 in 2009 edition).

3.17 New definition for **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 Revised definition for **organization**:

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

3.19 owner

No significant changes.

3.20 New definition for **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 There are no significant changes to the definition for **process**. However the definition has been made clearer:

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 Definition for **recorded material** has been simplified

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

3.23 Added wording "irrespective of time" to end of definition for **recording material**:

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

3.24 Revised definition for **recordings**:

electronic capture of images or data

3.25 remote centre

No change.

3.26 secure storage

No change.

3.27 New definition for **staff**

personnel involved in the management and operation of CCTV

3.28 Definition for **supervisor** has been simplified

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

No change.

3.30 Definition for **working copy** has been simplified:

copy of recordings which is used for review.

NOTE Also referred to as the "slave copy".

Some definitions from the 2009 edition have been deleted because they are no longer used and some of the definitions have been re-numbered.

4 PRINCIPLES AND MANAGEMENT OF A CCTV SCHEME

4.1 Objectives

The section on objectives has been expanded to cover 4.1.1 Use, 4.1.2 Effectiveness, 4.1.3 Transparency and 4.1.4 Standards.

4.1.1 Use

This clause contains revised requirements with emphasis on the CCTV scheme needing to have a clearly defined purpose in pursuit of a legitimate aim. This reflects the content of the Surveillance Camera Code of Practice.

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.

A new NOTE 1 draws attention to Principle 1 of the Surveillance Camera Code of Practice.

NOTE 2 is moved here from 4.2.1 of the 2009 edition.

4.1.2 Effectiveness

This clause contains new requirements reflecting the content of the Surveillance Camera Code of Practice.

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 identifies that 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 draws attention to Principle 11 of the Surveillance Camera Code of Practice and Principles 3 and 4 of the Data Protection Act 1998.

4.1.3 Transparency

This clause contains new requirements reflecting the content of the Surveillance Camera Code of Practice. The commentary on 4.1.3 states that 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.

The NOTE draws attention to Principle 3 of the Surveillance Camera Code of Practice and Principle 6 of the Data Protection Act 1998.

4.1.4 Standards

This clause contains new requirements reflecting the content of the Surveillance Camera Code of Practice.

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

NOTE 1 indicates that policies and procedures can apply not only to 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 draws attention to Principle 8 of the Surveillance Camera Code of Practice.

4.2 Policy

4.2.1 General

The content of this clause has been re-organised and is substantially the same as before.

There is a change to the 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.**

A new statement is included that **policies should reflect best practice and should be regularly reviewed**.

A new NOTE draws attention to Principle 5 of the Surveillance Camera Code of Practice and Principle 5 of the Data Protection Act 1998.

4.2.2 Policy and scheme review

The first paragraph has been re-worded as follows:

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.

An additional final paragraph has been added as follows:

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.

A new NOTE draws attention to Principles 2 and 11 of the Surveillance Camera Code of Practice and Principles 4 and 5 of the Data Protection Act 1998.

4.3 Procedures

Clause 4.3.2 on Methods for receiving and viewing data has been revised and expanded into clauses on 4.3.2 Information Security, 4.3.3 Access to data and 4.3.4 Supporting data.

4.3.1 General

The last paragraph from the 2009 edition has become the first paragraph of the 2015 edition and has been re-worded as follows:

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 draws attention to Principle 4 of the Surveillance Camera Code of Practice and Principle 7 of the Data Protection Act 1998.

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.

Other than this, the requirements are unchanged.

4.3.2 Information security

This is a new clause containing the following requirements:

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.

A new NOTE draws attention to Principles 6 and 9 of the Surveillance Camera Code of Practice and Principles 7 and 8 of the Data Protection Act 1998.

4.3.3 Access to data

This is a new clause containing the following requirements:

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 states that 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, 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 draws attention to the Freedom of Information Act 2000 and Principle 7 of the Surveillance Camera Code of Practice.

4.3.4 Supporting data

This is a new clause containing the following requirements:

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.

A new NOTE draws attention to the Regulation of Investigatory Powers Act 2000, Principles 7 and 12 of the Surveillance Camera Code of Practice and Principles 4 and 5 of the Data Protection Act 1998.

4.3.5 Use of temporary systems within the scheme

Previously 4.3.3 in the 2009 edition. No changes.

4.3.6 Annual report

Previously 4.5 in the 2009 edition.

There are no changes except for additional requirements to be included in the assessment of the scheme's performance as follows:

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.

A new NOTE 2 draws attention to Principle 10 of the Surveillance Camera Code of Practice.

4.3.7 Audit

Previously 4.4 in the 2009 edition.

There are no changes except for a new NOTE 2 that draws attention to Principle 10 of the Surveillance Camera Code of Practice.

4.4 Management and operation responsibilities

Previously 4.6 in the 2009 edition.

4.4.1 General

There are no significant changes except that NOTE 2 in the 2009 edition has been converted into normative text:

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.

A new NOTE 2 draws attention to Principles 4 and 5 of the Surveillance Camera Code of Practice.

4.4.2 Owner

There are no significant changes except that the owner is also responsible for **carrying out a privacy impact assessment**.

A new NOTE 3 draws attention to Principles 1 and 9 of the Surveillance Camera Code of Practice and Principle 2 of the Data Protection Act 1998.

4.4.3 Manager

There is a slight change to item g) where "data media" replaces "data medium, e.g. tapes;".

There are no other changes apart from the addition of two new notes.

NOTE 1 draws attention to the Surveillance Camera Code of Practice and Principles 4, 5 and 7 of the Data Protection Act 1998.

NOTE 2 draws attention to the Data Protection Act 1998 in relation to the data controller.

4.4.4 Supervisor

There is a slight, but important, change to the wording in the first paragraph of 4.4.4 whereby it is clearer that **the supervisor should bring to the immediate attention of the manager any matter affecting operation of the CCTV scheme, including any breach (or suspected breach) of the policy, procedural instructions, security of data or confidentiality**.

The list of items to be included in data recording systems has been shortened by removal of items a) the tape, or media, register; f) faults and maintenance records; and g) the security of data.

The focus is on items that need to be recorded/logged.

However the following item has been added to the list;

d) the maintenance log

A new NOTE 2 draws attention to Principles 4 and 7 of the Surveillance Camera Code of Practice and Principles 4 and 7 of the Data Protection Act 1998.

4.4.5 Operator

The first paragraph incorporates a change whereby the operator should work under the direction of the owner, manager or supervisor and in accordance with the policy and procedural practices.

The addition of the word "supervisor" is intended to reflect true circumstances.

This clause has been re-structured to some degree with re-organisation of the order of the text plus some changes to the text as follows:

become proficient has been replaced with **be proficient**.

This obviously reflects the need for operators to be proficient rather than at some later time.

The following sentence has been added:

Operators should have been appropriately screened for handling personal data and images.

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

The following paragraph has been added:

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

The wording **be trustworthy** has been deleted from a different paragraph.

This does not mean that operators should not be trustworthy. However it is difficult to detect lack of trustworthiness until something has happened. Therefore trustworthiness was not easily auditable.

4.4.6 Contractor

There are no significant changes. However reflecting the changes to the Annexes:

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.

The NOTE draws attention to Principles 7 and 8 of the Data Protection Act 1998 [1].

5 PERSONNEL

5.1 Security screening

There are no significant changes other than the inclusion of the word **images** in relation to employment that might involve the acquisition of such information.

This emphasises the significance of "images" in the context of CCTV and the need to security screen all personnel whose employment involves access to images as well as other kinds of information.

5.2 Recruitment and selection

There are no changes.

5.3 Training

The previous sub-clause headings 5.3.1 (General) and 5.3.2 (Plan) have been removed to leave the main heading (5.3) and the order of the text has been changed.

The 2009 edition used the terms "employees" and "staff" and these were not defined. In order to provide a clearer set of requirements the term "staff" has been defined (see 3.27 in the 2015 edition) and the term "employees" has been withdrawn.

The new clause 5.3 opens with a revised paragraph as follows:

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

The 2009 edition stated that there **should be a formal training plan that includes information on the following** and in a sense it was difficult to draw the line in terms of what formal means. This position has been simplified to **Training should include the following** and then there is a list of items to be included. The list of training items is the same as in the 2009 edition apart from the following:

Expansion of item e):

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];

Removal of item f):

f) the progression to nationally recognized qualifications, e.g. NVQ, SVQ, City & Guilds;

The NOTE has been revised:

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

The following statement has been deleted:

"A minimum period of training should be stated that is appropriate to ensure at least the minimum competence to carry out the specified duties."

This has been replaced with a clearer statement: **The period of training should be sufficient to ensure that staff are able to carry out the specified duties**.

NOTE 1 in the 2009 edition has been converted to normative text:

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.

A new NOTE 2 draws attention to the Criminal Procedure and Investigation Act 1996, 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

References to CCTV Image Receiving Centre have been replaced with **CCTV control centre**.

The following change of text has been made:

Toilet and kitchen facilities for CCTV control centre staff should be provided.

The standard does not stipulate these facilities need to be inside the CCTV control centre.

There is a new second paragraph which states:

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.

This would include means for raising the alarm in case of a medical emergency affecting a lone CCTV control centre operator.

There is a change of text from "have the means for direct communication with the law enforcement agencies" to **have the means of communication with the emergency services**.

This avoids the need to interpret the meaning of "direct".

The need to sign a visitors' log now applies to entering **and exiting** the CCTV control centre.

The standard now states law enforcement agency officers **should** be granted the right to enter the CCTV control centre at any time for liaison and security objectives.

The following note has been added:

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

This means law enforcement agencies must adhere to the access protocols just like any other party.

6.2 Ergonomics

There are no changes apart from an update to Note 2 which now draws attention to the Equality Act 2010.

6.3 Health and safety

The first paragraph has been re-worded as follows:

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

The main change here is the requirement to document shift patterns and show how sufficient breaks are included.

A new NOTE 2 draws attention to the Health and Safety (Display Screen Equipment) Regulations 1992, Regulation 4.

A new NOTE 3 draws attention to the Working Time (Amendment) Regulations 2002.

7 INCIDENT HANDLING

The title has been changed from "Response" in the 2009 edition to "Incident handling" to reflect the correct scope of this section of the standard.

Clause 7.6 "Result of a successful response to the incident" has been deleted because the success or otherwise of the response is usually outside the control of the CCTV control centre.

7.1 General

This clause, previously called "Guiding principle", has been simplified:

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

There are no significant changes.

7.3 Incident response

The title has changed from "Making the response".

The text has been simplified:

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

A new NOTE states, depending on the incident, the response might be by emergency services, private security, roadside assistance, etc.

7.4 Timescale of the incident notification

The second paragraph has been deleted.

7.5 Incident observation and/or recording

The title has changed from "When observation and/or recording is needed".

The text has been simplified:

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

A new NOTE states 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

The word "surveyed" has been changed to "viewed".

The NOTE now draws attention to Principle 6 of the Data Protection Act 1998 and Principle 2 of the Surveillance Camera Code of Practice.

8.2 Disclosure of data

8.2.1 General

A new NOTE draws attention to BS ISO 27001 for guidance on information security.

8.2.2 Request to disclose data

There are no significant changes.

NOTE 1 has been converted into a commentary.

A new NOTE 3 draws attention to Principle 6 of the Data Protection Act 1998 and Principle 7 of the Surveillance Camera Code of Practice.

8.3 Subject access disclosure (a named subject)

There are no significant changes.

NOTE 1 has been converted into a commentary.

The new NOTE 1 draws attention to Principle 6 of the Data Protection Act 1998 and Principle 7 of the Surveillance Camera Code of Practice.

The last paragraph of the 2009 edition has been merged with NOTE 3 in the 2009 edition to create NOTE 2 in the 2015 edition as follows:

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

There are no significant changes.

A new NOTE draws attention to Principle 6 of the Data Protection Act 1998 and Principle 7 of the Surveillance Camera Code of Practice.

9 RECORDED MATERIAL MANAGEMENT

Clause 9.2 regarding Quality has been deleted.

9.1 General

New requirements have been added as follows:

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.

The sentence about the electronic document management system conforming to BIP 0008-1, BIP 0008-2 and BIP 0008-3 has been converted into NOTE 1.

The following text has been deleted:

"Data should not be released to organizations outside the ownership of the CCTV scheme, other than under guidelines referring to the release of information for the purposes of identifying alleged offenders or witnesses, in accordance with the particular CCTV control room's policy and procedure (see Clause 8)."

The reason is that privacy and disclosure issues are dealt with under clause 8.

The original NOTE 1 from the 2009 edition has been deleted because "hard copy print" is defined.

A new NOTE 2 draws attention to Principle 5 of the Data Protection Act 1998 and Principle 6 of the Surveillance Camera Code of Practice.

9.2 Media use, storage and disposal

The last paragraph of 9.3 of the 2009 edition has been moved to become the first paragraph of 9.2 of the 2015 edition.

The text recommending reuse of tapes a maximum of 12 times has been converted into a NOTE:

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

9.3 Recorded material register

Clauses 9.4.1 "Videotape" and 9.4.2 "Digital register" have been merged under the main heading "recorded material register" to create single set of requirements for all media.

The revised 9.3 opens with the following requirements:

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.

Also NOTE 1 has been deleted.

9.4 Making recordings

There are no significant changes.

The word "efficiently" has been changed to "correctly" so 9.4 a) reads as follows:

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

The last paragraph in the 2009 edition has been split into a requirement and a NOTE.

The requirement reads:

All documentation should be auditable.

The NOTE reads:

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

There are no changes.

10 DOCUMENTATION

10.1 General

The final paragraph of 10.1 of the 2009 edition has been converted into a NOTE as follows:

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

There are no significant changes.

The word **contractual** has been deleted from item 10.2 d).

10.3 Administrative documents

The NOTE has been converted to a commentary.

A new NOTE draws attention to Principle 6 of the Data Protection Act 1998 and Principle 7 of the Surveillance Camera Code of Practice.

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

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

(previously Annex A of BS 7958:2009)

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.

Guidance on the implementation of BS 7958:2015 Annex C is given in NSI Technical Bulletin 0030.

Contractors that demonstrate compliance with Annex C, and also satisfy the relevant NSI criteria for approval, will be approved for the following scope:

"The Provision of Security Screened and Trained Personnel to Conduct Closed Circuit Television Monitoring Activities".

ANNEX D (normative)

Management and operation of CCTV traffic enforcement cameras

(previously Annex B of BS 7958:2009)

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].

Guidance on the implementation of BS 7958:2015 Annex D will be given separately in another NSI Technical Bulletin.

Organisations that demonstrate compliance with Annex D, and also satisfy the relevant NSI criteria for approval, will be approved for the following scope:

"The Management and Operation of CCTV Traffic Enforcement Cameras".

ANNEX E (normative)

Contracted remote CCTV control centre responsibilities within BS 7958

(previously Annex A of BS 7958:2009)

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.

Guidance on the implementation of BS 7958:2015 Annex E will be given separately in another NSI Technical Bulletin.

Organisations that demonstrate compliance with Annex E, and also satisfy the relevant NSI criteria for approval, will be approved for the following scope:

"The Provision of Contracted Remote CCTV Control Centre Services".

Bibliography

The following documents are additions to the Bibliography:

Standards publications

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

Other publications

[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.

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

[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.

[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.

[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.