Corporate procedure
Closed Circuit Television (CCTV) Code of Practice

Issue sheet

<table>
<thead>
<tr>
<th>Document reference</th>
<th>PFM 023</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document location</td>
<td>P&amp;FM Team</td>
</tr>
<tr>
<td>Title</td>
<td>CCTV Code of Practice</td>
</tr>
<tr>
<td>Author</td>
<td>I. Heywood</td>
</tr>
<tr>
<td>Issued to</td>
<td>NHSBSA Hub</td>
</tr>
<tr>
<td>Reason issued</td>
<td>Provides business wide guidance on CCTV within the NHSBSA.</td>
</tr>
<tr>
<td>Last reviewed</td>
<td>11/11/2015</td>
</tr>
<tr>
<td>Date of Equality Assessment</td>
<td>11/11/2015 (equality statement added)</td>
</tr>
<tr>
<td>Date of Fraud Review</td>
<td>Not required</td>
</tr>
</tbody>
</table>

Revision details

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Amended by</th>
<th>Approved by</th>
<th>Details of amendments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------------</td>
<td>------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Scope</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>References</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Introduction</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>CCTV - a strategy</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Core aims of CCTV</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>The code of practice for the NHSBSA</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1</td>
<td>Introductory section</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2</td>
<td>Purpose statement</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.3</td>
<td>Data protection implications</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.4</td>
<td>Changes to the code</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.5</td>
<td>Responsibility of the owner of the scheme</td>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.6</td>
<td>Management of the system</td>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Installation</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.1</td>
<td>Consultation</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.2</td>
<td>Sound</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.3</td>
<td>Change</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.4</td>
<td>Replica cameras</td>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>Accountability</td>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.1</td>
<td>The public</td>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.2</td>
<td>Public information</td>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.3</td>
<td>This code of practice</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.4</td>
<td>Annual statistical report</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>Assessment of the scheme and the code of practice</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.1</td>
<td>Evaluation</td>
<td>13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.2</td>
<td>Monitoring</td>
<td>13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.3</td>
<td>Audit</td>
<td>14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>Staff /employees</td>
<td>14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td>Complaints</td>
<td>15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>Breaches of the code including those of security</td>
<td>15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td>Control and operation of cameras</td>
<td>16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.</td>
<td>Access to and security of monitors/controlled area</td>
<td>16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.1</td>
<td>Monitors</td>
<td>17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------</td>
<td>------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.2</td>
<td>Controlled area</td>
<td>17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.3</td>
<td>Supervision and audit</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.4</td>
<td>Log books</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.5</td>
<td>Health and safety</td>
<td>19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>Discs and recorded data</td>
<td>19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.1</td>
<td>Statement of intent</td>
<td>20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.2</td>
<td>Ownership</td>
<td>20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.3</td>
<td>Accurate recording</td>
<td>20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.4</td>
<td>Use of discs</td>
<td>20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.5</td>
<td>Cataloguing, storage, and recording of use of discs</td>
<td>21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.6</td>
<td>Evidential use of recordings</td>
<td>21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.7</td>
<td>Police access to discs</td>
<td>21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16.</td>
<td>Data Protection Subject Access Request</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17.</td>
<td>Still digital prints (photographs)</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.</td>
<td>Dealing with incidents</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19.</td>
<td>Glossary</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19.1</td>
<td>Audit</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19.2</td>
<td>Evaluation</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19.3</td>
<td>Monitor</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19.4</td>
<td>Owner</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19.5</td>
<td>Operator</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19.6</td>
<td>Partnership</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19.7</td>
<td>Recorded data</td>
<td>23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19.8</td>
<td>Scheme</td>
<td>23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19.9</td>
<td>System</td>
<td>23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19.10</td>
<td>Disc</td>
<td>23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20.</td>
<td>Revision history</td>
<td>23</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1. Scope

1.1 This procedure applies to all sites controlled by the NHS Business Services Authority (NHSBSA). The aim of this procedure is to provide guidance on the Closed Circuit Television (CCTV) systems used within the business and is based on the government publication “A Code of Practice for CCTV” (www.ico.gov.uk).

1.2 In applying this code of practice, the NHSBSA shall have due regard for the need to eliminate unlawful discrimination, promote equality of opportunity, and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic.

2. References

In the picture: A data protection code of practice for surveillance cameras and personal information (www.ico.org.uk)
Data Protection Act 1998
Human Rights Act 1998
Information Security Incident Reporting Procedure
Police and Criminal Evidence Act
The Criminal Procedure (Scotland) Act 1995
The Criminal Procedures and Investigations Act

3. Introduction

3.1 The use of Closed Circuit Television (CCTV) is viewed by the NHSBSA as a key element in its promotion of a safer working environment. CCTV systems are in place / being developed throughout many areas of the business.

3.2 The NHSBSA currently has CCTV Surveillance at:

- Newcastle upon Tyne
  - Bridge House - NE1 6SN
  - Stella House - NE15 8NY
  - Benton Warehouse - NE12 9UP

- Bolton, Middlebrook
  - Ridgway House - BL6 6PQ

- Wakefield
  - Wakefield House - WF1 3UB
3.3 This code sets out the minimum standards that are expected of all employees, authorised agents and users operating CCTV systems within the NHSBSA. Our aim is at all times to balance the individual’s right to privacy with the organisation’s responsibility to provide a safe and secure environment.

3.4 NHSBSA Property & Facilities Management and Information Governance Team shall be responsible for implementing training to ensure that data protection principles, matters of confidentiality and operational procedures are familiar to all employees, authorised agents and users operating surveillance systems.

3.5 The efficient operation of CCTV rests with the standards contained within this code of practice. It should be considered as a benchmark for good practice that shall ensure accountability and command public confidence.

3.6 Further advice and guidance on any aspect of the Code of Practice can be obtained from:

- In the picture: A data protection code of practice for surveillance cameras and personal information

3.7 This should be read in conjunction with the guide to the 12 principles:


3.8 Ownership of all recorded data remains at all times the property of the NHSBSA.

4. **CCTV - a strategy**

4.1 CCTV should not be regarded as the solution to every problem of crime or safety within the NHSBSA. However, there is no doubt that the effects of such schemes can have considerable bearing in promoting a safer working environment and the reduction of crime and disorder in designated areas. The true potential of CCTV rests with a strategy that is proactively developed by the NHSBSA, the Police and other stakeholders or users of the buildings, and which address a range of safety issues.

4.2 In developing such a strategy, available resources can contribute to achieving expressed aims and objectives, but success to such an achievement cannot be undertaken by CCTV alone. The uses of CCTV are wide and varied, but in broad terms, its use contributes to the following objectives:
• detecting, preventing or reducing the incidence of property crime and offences against the person
• improving communications and the operational response of security patrols in and around the NHSBSA premises

5. Core aims of CCTV

In tackling any of the above objectives, all relevant bodies will have to be consulted upon and considered with the aim of establishing an effective scheme that has full staff and public support. Any developments undertaken by the NHSBSA to introduce CCTV shall be based upon the following core aims:

• to encourage the legal, efficient and effective use of the technology available
• to ensure that CCTV systems strengthen the NHSBSA’s position for compliance with current and future data protection and human rights legislation
• to instill and maintain public confidence in the use of the CCTV system
• to act in partnership with police and other agencies / businesses in the approach to CCTV, thereby increasing public confidence through open and effective partnerships
• to promote the adoption of clear, well-recognised standards for CCTV that command public confidence
• moreover, these aims should complement the key principles behind any scheme, notably data protection, human rights, public interest, accountability and privacy

6. The code of practice for the NHSBSA

To ensure a good standard is set for CCTV operation, the NHSBSA has adopted and amended this code of practice from the Government information.

6.1 Introductory section

6.1.1 The scheme(s) established within the properties and associated buildings owned/leased by the NHSBSA have been commissioned in accordance with the Core Aims identified earlier in this document. For the purposes of the Data Protection Act 1998 the System Controller for the system(s) is:

NHS Business Services Authority.
Stella House
Goldcrest Way
Newburn Riverside
Newcastle upon Tyne
NE15 8NY
6.1.2 Others that have responsibility for the management, administration and operation of the system are:

<table>
<thead>
<tr>
<th>NHSBSA title</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Executive</td>
<td>Data Controller</td>
</tr>
<tr>
<td>Head of Internal Governance</td>
<td>Data Protection Officer</td>
</tr>
<tr>
<td>Local Security Management Specialist</td>
<td>Nominated Representative</td>
</tr>
<tr>
<td>Security staff</td>
<td>System operation</td>
</tr>
</tbody>
</table>

6.1.3 The CCTV system(s) briefly comprises of the following primary items of equipment:

- colour cameras
- multiplexed output monitors
- remote site monitors
- spot monitors
- monitor in the reception areas
- monitor in building exteriors
- digital recorders for multiplexed output
- spot recording digital recorders

It should be noted that the use of automatic number plate recognition (ANPR), drone cameras and body worn camera are not in use.

6.1.4 The system runs on a 24 hour, 7 day a week basis, with automatic summer and winter time settings and all recorded data remains the sole copyright of the NHSBSA.

6.2 Purpose statement

6.2.1 The NHSBSA have considered several principles in relation to this purpose statement, notably that the scheme shall be operated fairly, within applicable law, and only for the purpose for which it is established or which are subsequently agreed in accordance with the code of practice.

6.2.2 The CCTV system shall at all times be operated with due regard to the privacy of the individual. Public interest in the scheme shall be recognised by ensuring the security and integrity of operational procedures.

6.2.3 Participation in the scheme by the NHSBSA (and other organisations) is dependent at all times upon their willingness to comply with the code of practice and to be accountable under the code of practice.
6.2.4 Therefore the purposes for which the scheme(s) are established reflect those established within the Data Protection Act 1998 namely crime prevention, crime detection and the promotion of public safety within the boundary of the properties owned and or controlled by the NHSBSA.

6.2.5 The key objectives being:

- the reduction or negating of criminal activity within the areas owned or controlled by the NHSBSA
- particularly, but not exclusively, physical violence against members of staff
- assistance with risk management

6.3 Data protection implications

6.3.1 The NHSBSA is aware of the legal responsibilities placed upon it by the introduction of the Data Protection Act 1998 and the Human Rights Act 1998.

6.3.2 In accordance with the requirements of the Data Protection Act 1998 the CCTV system along with all other data collection methods used by the NHSBSA has been registered or “notified” to the Data Protection Commissioner.

6.3.3 The CCTV systems shall be operated in full compliance with this current code of practice.

6.3.4 The NHSBSA shall display appropriate signs to notify visitors and users of the various premises of the presence of CCTV recording equipment. These signs shall carry the necessary information prescribed in the Information Commissioner’s Code of Practice.

6.3.5 Further information in respect of data protection issues can be obtained from the Head of Internal Governance on: 0191 203 5484

6.4 Changes to the code

Revision and changes to this code of practice may occur during the life of a CCTV scheme.
6.5 Responsibility of the owner of the scheme

6.5.1 The NHSBSA being the Owner and Data Controller has prime legal responsibility for compliance with the purposes and objectives of the scheme, for management and security of the scheme, and the protection of the interests of the public and of the individual.

6.5.2 In establishing the CCTV systems with ownership and control, the NHSBSA shall:

- consult with and provide information to the Information Governance and Security Group and other users of the buildings and facilities including where appropriate the public, about the operation of the scheme and about any proposed changes to the scheme or the code of practice
- where appropriate seek agreement through the letting of contracts to companies and organisations involved with the NHSBSA to the use of CCTV in accordance with this Code of Practice
- provide access to the appropriate “public” documentation to the above groups
- be responsible for the introduction and implementation of the code of practice, and for ensuring compliance with operational guidance derived from the code of practice
- comply with requirements for accountability

6.6 Management of the system

6.6.1 Effective management of the scheme requires that the following staff shall have day-to-day management of a scheme and the requirements of a code of practice. Local Security Management Specialist and the Head of Internal Governance (remote premises should report directly to the above team).

6.6.2 Where appropriate liaison with the police shall be undertaken through, but not exclusively limited to the local police constabulary appointed Crime Prevention Officer.

6.6.3 Access to all the data held and the controlled area should comply with specific guidelines, and be recorded and monitored.

6.6.4 The operational documentation required to run a scheme must be developed from and specifically linked to the code of practice.
7.0 Installation

7.1 Consultation

7.1.1 Consultation is vital to the process of installation. All relevant concerns should be taken into account with the aim of establishing an effective scheme, which has the full support of staff, visitors and users of the NHSBSA.

7.1.2 The NHSBSA shall ensure that consultation is effective, fair and open to all sections of the Authority. Expectations are often raised by the proposed installation of schemes, and the staff and public should be properly informed about the purpose of the CCTV installation in order to respond to consultation.

7.1.3 Where the NHSBSA are the responsible body for installing the scheme, installation shall be carried out only after consultation.

7.1.4 Consultation shall be undertaken with bodies as appropriate such as recognised employee representatives, businesses, and others on the issues raised by the scheme prior to installation.

7.1.5 Where cameras are to be installed in buildings under the control of the NHSBSA, the business shall consult with occupiers. Primary concern must take into account the Human Rights Act 1998 and the Data Protection Act 1998.

7.2 Sound

Sound shall not be recorded.

7.3 Change

7.3.1 The NHSBSA wants to keep any CCTV system at an appropriate level of technical and physical standards.

7.3.2 Before the introduction of major technological change that may have a significant effect upon the capacity of the system, the implications shall be fully assessed in relation to the purpose and key objectives of the scheme and, if appropriate, be the subject of wider consultation.

7.3.3 The introduction of technological change shall be linked to the assessment process adopted under the Code of Practice and the precise definitions made of the standard which it is hoped to achieve.
7.3.4 Where the scheme is established by a partnership, the informed agreement of all partners must be obtained before the introduction of such technological change.

7.3.5 The consideration and/or introduction of any technological change must be reported in the annual report.

7.4 Replica cameras

7.4.1 The NHSBSA is wary of making false claims about the effectiveness of schemes to avoid raising expectations unduly. In the long-term interests of CCTV, public confidence may be lost if failure to respond to an important incident is attributed to a replica camera.

7.4.2 Therefore NHSBSA agree that public confidence afforded by the scheme should be based on effective operating cameras and replica cameras shall not be used.

8.0 Accountability

8.1 The public

8.1.1 NHSBSA recognises the requirement for a well-defined structure of accountability to the staff, public and other users of the Authority’s facilities.

8.1.2 Copies of the Code of Practice and particulars of the complaints system and a standard subject access request form shall be available in accordance with the Code of Practice and with the data subject rights of section 7 of the Data Protection Act 1998.

8.1.3 The Code of Practice can be viewed on request and Data Subject Access forms are also be available (see link here). Anyone wishing to acquire a copy of the Code of Practice or to request further information with regard to accessing the recorded Data under the Data Protection Act 1998 should be directed to contact the Head of Internal Governance in writing to the Stella House office.

8.2 Public information

8.2.1 There is a need for continued public understanding and acceptance of CCTV, which involves providing a high quality of information. The recording and retention of images (data) of people in public places shall be undertaken fairly and lawfully in accordance with the Human Rights Act 1998 and the Data Protection Act 1998.
8.2.2 For this reason, the purpose for which information is obtained by a system should be known, and information should not be used for any purpose that has not been disclosed to the public.

8.2.3 People should be aware that their image is being recorded and that the identity of the owner and purpose of the scheme should be made known.

8.2.4 The provision of information to staff, other users and members of the public that the images of individuals are being recorded is an important aspect of the data protection principles, therefore signage to this effect shall be displayed as sufficient.

8.2.5 To this end the NHSBSA shall ensure that:

- cameras should not be hidden but as far as is consistent with the purposes of the scheme be placed in public view
- all signs must be fit for purpose and careful consideration shall be given to placement, size, opportunity to view etc.
- the signs shall indicate that CCTV cameras are operating and shall be displayed at the perimeter of the area covered by the scheme and at other key points
- the signs shall inform the public that cameras are in operation and allow people entering the area to make a reasonable approximation of the area covered by the scheme
- the signs shall identify the owner by name, purpose of a scheme and give a daytime contact telephone number

8.2.6 This is an essential requirement of the Data Protection Act 1998 (Principle 1). A serious breach of the Act is committed if it is not complied with and public knowledge of the scheme shall be limited and an important safeguard lost.

8.3 This code of practice

This Code of Practice is a public document and shall be available for inspection. The availability of the Code of Practice and subject access forms shall be highlighted in connection with any publicity arranged for the scheme.

8.4 Annual statistical report

The provision of the annual statistical report is a minimum requirement. Information should include illustrations of any statements that are made about the scheme, including providing percentages relating to reduction of crime,
incidence of crime, arrest or convictions, subject access requests (not police) and complaints against the system.

9.0 Assessment of the scheme and the code of practice

Assessment involves evaluation, monitoring, audit, and inspection of the operation of the scheme and of the code of practice.

9.1 Evaluation

9.1.1 Effective independent evaluation of the scheme is essential to identify whether the purposes of the scheme are being complied with, and whether objectives are being achieved.

9.1.2 The NHSBSA is responsible for ensuring that the scheme is evaluated at the outset in regard to baseline conditions and periodically thereafter.

9.1.3 Evaluation of the scheme should include as a minimum:

- baseline statement of conditions of crime and safety in the area
- assessment of impact upon crime:
- assessment of neighbouring areas without CCTV
- the views of the public
- operation of the Code of Practice
- whether the purposes for which the scheme was established still exist
- the results of evaluation should be published
- resources committed to the scheme annually should include the costs of evaluation
- the results of evaluation should be taken into account in the future functioning, management and operation of the scheme
- complaints against the system
- number of Data Protection Act 1998 subject access request
- a monitoring and evaluation group should be established

9.2 Monitoring

Purpose of monitoring is to ensure the compliance with the requirements of the Code and operational guidance. The individual(s) with day to day responsibility for the scheme shall continuously monitor the operation of the scheme and of the implementation of the Code of Practice and associated operating procedures.
9.3 Audit

Audit is needed to provide an account of the operation of the scheme and should include examination of controlled area records, disc histories, and the content of recorded discs, digital prints and be undertaken on a sufficiently regular basis to provide an effective safeguard for the scheme. The audit shall be undertaken in full compliance with the Data Protection Act 1998 and the informed of the Data Controller or Nominated Representative.

9.4 Inspection

Ongoing public confidence in the scheme should be addressed by including an independent element in assessment.

10. Staff / employees

10.1 The following principles should be observed where staff are involved in the operation of CCTV:

- staff should meet high standards of probity
- well-trained accredited and responsible staff with good working conditions is essential for the proper and effective working of the scheme
- all procedures concerning staff should accord with employment practice incorporating equal opportunities standards
- systems providing security and safeguards for recorded data and the system itself are the core of good management of the scheme

10.2 To this end the operation of CCTV by the NHSBSA has:

- an effective and fair system of recruitment and selection of staff which includes measures to ensure that the selection process provides for thorough validation of the suitability of candidates
- identified that staff should ideally hold a valid Security Industry Association (SIA) licence for the operation of CCTV on appointment or be offered and be capable of meeting these and other in-service training requirements
- a disciplinary procedure, which incorporates compliance with the Code of Practice and operational requirements and makes plain the risk to staff in the event of breaches of the Code of Practice or misappropriation of recorded data
- a suitable employee's declaration of confidentiality which can be enforced during and after termination of employment
- systems of monitoring and supervision that ensure compliance with the Code of Practice and operational guidelines
11. Complaints

11.1 To obtain universal recognition, the code of practice must address the interests of all who may be affected by it, and not just be confined to the interests of the NHSBSA, or the needs of the criminal justice system. The code of practice does include checks and sanctions, and shall only be effective if it does so.

11.2 Schemes covered by the Data Protection Act 1998, provide individuals with certain remedies including the right to complain to the Data Protection Commissioner.

11.3 Complaints shall be included in the annual report providing information on the number of complaints received, of those complaints that have been substantiated, and any action taken to remedy the complaint. Remedies shall vary according to the complaints received.

11.4 It may be appropriate to allow the complainant access to the controlled area in certain limited circumstances but only with the Data Controller’s informed consent. The Data Protection Act 1998 may well prevent this as this could be deemed unauthorised processing.

11.5 This could be done to allow a complainant to confirm whether residential premises can be seen on a particular camera, or to be satisfied that a remedy to prevent oversight by the camera has proved effective.

11.6 Any complaints, which offer suggestions to policy changes, should be referred to the monitoring and evaluation group.

11.7 To this end the NHSBSA shall publish information about the manner in which an individual can make a complaint or Data Subject Access request about any aspect of the scheme.

12. Breaches of the code including those of security

12.1 Prime responsibility for the Code of Practice and for security rests with the NHSBSA. This responsibility includes ensuring that breaches are investigated and remedied. Professional qualifications relevant to the appointment of an individual to investigate a serious breach shall depend upon the subject matter of the investigation, but would include relevant technical and legal knowledge.

12.2 Responsibility for physical security shall be with the Head of Property.

12.3 Sufficient resources and facilities shall be made available to enable that responsibility to be fulfilled.
12.4 Breaches of the Code of Practice and of security must be subject to proper investigation by, in the first instance, the person appointed to conduct inspections. This person shall be responsible for making recommendations to the NHSBSA to remedy any breach which is proved.

12.5 Where a serious breach occurs, the NHSBSA shall appoint an individual with relevant professional qualifications independent from the operation of the scheme to investigate the breach and to make recommendations to the NHSBSA on how the breach can be remedied.

13. Control and operation of cameras

13.1 Information recorded should be accurate, adequate, relevant and not exceed that necessary to fulfil the purpose of the scheme. Information recorded should be obtained fairly and in accordance with the provisions of the code of practice on privacy.

13.2 NHSBSA shall ensure that:

- operators of camera equipment shall act with the utmost probity
- only staff with responsibility for using the equipment shall have access to operating controls
- all use of the cameras shall accord with the purposes and key objectives of the scheme as developed in training and specific operational instructions to staff, and shall comply with the code of practice
- cameras shall not be used so as to look into private property including residential establishments within the grounds of the NHSBSA premises (the NHSBSA recognises it is under a legal obligation to adopt operational procedures and technological measures that impose restraints upon the use of cameras in connection with private premises
- camera operators shall be subject to supervision procedures that are sufficient to ensure compliance with this part of the code of practice
- all camera operators shall be made aware that recordings are subject to routine audit and inspection and that they shall be required to justify their interest in a member of the public or premises

14. Access to and security of monitors/controlled area

Only those with a legitimate reason to do so shall operate or view the equipment and recorded data, whether recordings or digital prints. Regard must be had to the provisions of the Code of Practice on privacy.
14.1 Monitors

14.1.1 Access to view monitors, whether to operate the equipment or to view the images is limited to staff with that responsibility. Others may be permitted, but only with the Local Security Management Specialist’s informed consent.

14.1.2 A controlled area occurrence book should record staff on duty each shift, and the names of any persons or groups, that have been authorised by the individual with day to day responsibility for the scheme, to have access to the controlled area and/or view the monitors.

14.1.3 A competent operator shall be present during the operation of monitors. If monitors are to be left unattended, the area in which they are kept shall be secured against unauthorised entry.

14.1.4 Public access to or the demonstration of monitors and related equipment shall not be allowed except for lawful purpose, proper and sufficient reasons but only with the Local Security Management Specialist’s informed consent.

14.2 Controlled area

14.2.1 Visits approved by the NHSBSA may include demonstrations of the controlled area to those considering the relevance of CCTV in other areas, although care must be exercised to ensure that other provisions of the code of practice are observed during such visits.

14.2.2 Visits may also be allowed for the purpose of authenticated research and demonstration purposes but only with the Head of Internal Governance’s informed consent.

14.2.3 Complainants may also be allowed access in some circumstances.

14.2.4 The NHSBSA shall ensure that arrangements for the controlled area include the following requirements to ensure that the controlled area is secure at all times.

14.2.5 Routines and procedures and any other facilities necessary to ensure that the controlled area is protected from unauthorised access.

14.2.6 Records are kept of all access to the controlled area, recording details of the individual concerned, and time of arrival and departure.
Operation times and the numbers of staff on shift are clearly defined and complied with.

14.2.7 Access to the controlled area will normally be restricted to operating staff and their managers according to pre-arranged shifts and on production of valid identification.

14.2.8 Technical repairs, cleaning and similar tasks should be carried out in controlled circumstances.

14.2.9 Access by visitors shall be carefully defined and be the responsibility of NHSBSA but only with the Local Security Management Specialist informed consent after consultation with the Head of Internal Governance.

14.2.10 Unauthorised access to the controlled area may constitute a breach of the Data Protection Act 1998 and must be reported to the Head of Internal Governance and the Local Security Management Specialist.

14.2.11 Close liaison between the Police and the NHSBSA is recommended and encouraged. Police visits will usually be prearranged, and may simply be to collect / return discs or may be to interview staff. Other visits by the Police may take place from time to time in accordance with the provisions of the code of practice. The police may be involved in a multitude of purposes in relation to the day to day responsibility for schemes in compliance with other provisions of the code.

14.2.12 Independent inspectors appointed under the code of practice may visit without prior appointment. Inspections must be carried out in full compliance with the Data Protection Act 1998.

14.3 Supervision and audit

The NHSBSA shall ensure that security procedures on access to the controlled area must be maintained and strictly adhered to. Access must be monitored and all concerned should know that security procedures on access to the controlled area are included in the regular audit.

14.4 Log books

The NHSBSA shall ensure that a Log Book shall be maintained on the basis of date and time of day throughout operations and brief details given of all incidents within the controlled area, including particulars of visits and operational telephone calls.
14.5 Health and safety

14.5.1 The NHSBSA keep abreast of developments in the field of controlled area management. The operating environment, lighting, positioning of CCTV monitors, ventilation, and number of viewing hours, will have a relationship to operator efficiency. Compliance with health and safety legislation is a requirement of the code of practice.

14.5.2 Further health and safety advice on any part of scheme or can be requested via the NHSBSA Safety, Health and Environment (SHE) Team at:

nhsbsahealthandsafety@nhs.net

15. Discs and recorded data

Recorded data can relate to discs, DAT, compact disk, computer disk, digital print and film or any mechanism for storing images, which can be viewed or processed after the event. The most popular medium of CCTV coverage is disc. Several legally enforceable principles apply to this section, notably:

- recorded data may be used in court as evidence (It must be of good quality, and be accurate in content)
- recorded data must be treated according to defined procedures to provide continuity of evidence and to avoid contamination of the evidence
- appropriate security measures shall be taken against unauthorised access to, alteration, disclosure or destruction, and against accidental loss or destruction of recorded data
- recorded data should be held only for the purposes provided by this code of practice
- information recorded should be accurate, adequate, relevant and not exceed that necessary to fulfil the purposes and key objectives of the scheme
- recorded data shall be kept no longer than is necessary for the purposes and key objectives of the scheme (It must then be safely destroyed)
- members of the public must be confident that information recorded about their ordinary activities in the area covered by the cameras is treated with regard to their individual privacy
- only data required as evidence for a police or internal investigation(s) shall be retained (These recording(s) should only be retained for the duration of the investigation)
15.1 Statement of intent

In accordance with the above principles, the NHSBSA adopts the following as a statement of intent on use of and access to recorded data:

- recorded data shall be used only for the purposes defined in the Code of Practice
- access to recorded data shall only take place as defined in the Code of Practice
- In particular, recorded data shall not be sold or used for commercial purposes or the provision of entertainment
- the showing of recorded data to the public shall only be allowed in accordance with the law; either in compliance with the needs of the police in connection with the investigation of crime, which shall be conducted in accordance with the provisions of the Police and Criminal Evidence Act, The Criminal Procedures and Investigations Act and The Criminal Procedure (Scotland) Act 1995; or in any other circumstances prescribed by law

15.2 Ownership

Ownership of recorded data remains at all times the property of the NHSBSA.

15.3 Accurate recording

15.3.1 Recording equipment should be checked daily to ensure it is in good working order and that the date and time shown is correct.

15.3.2 A system check should be made daily to ensure pre-recorded data can be viewed.

15.4 Use of discs

15.4.1 Data shall be retained for a maximum of 30 days before being overwritten. Some situations may require 90 days (for example, where passport, credit card and bank account details are stored and/or viewed).

15.4.2 Discs required for evidential purposes must be separately indexed and securely stored separately to avoid accidental re-use.

15.4.3 Discs shall be disposed of in a secure manner through degaussing and physical destruction.
15.5 Cataloguing, storage, and recording of use of discs

15.5.1 Discs must be individually and uniquely identified and labeled.

15.5.2 A register must be maintained giving exact date and time of each use of each disc recorded, to whom the disc was issued, why it was required, the reason for its removal, and the estimated date it would be returned or destroyed.

15.5.3 The disc register must be stored securely.

15.6 Evidential use of recordings

15.6.1 Any disc that is provided for evidential purposes must be of proven integrity.

15.6.2 Staff shall be required to provide the police with statements and supporting material required for evidential purposes.

15.6.3 When internal CCTV evidence is required, depending on the type of investigation being carried out, the disc shall be held with the body holding the investigation (for example disciplinary – HR).

15.7 Police access to discs

15.7.1 Police may apply for access in accordance with a legal provision and with any agreement made with the NHSBSA where the police reasonably believe that access to specific recordings are necessary for the investigation and detection of a particular offence or offences or for the prevention of crime.

15.7.2 Discs provided to the police shall at no time be used for anything other than the purpose specified and identified when the copy disc is released to the police by the controlled area.

15.7.3 Arrangements may be made from time to time for a police officer appointed in accordance with liaison arrangements to visit the controlled area and confirm that agreed procedures are being followed.

15.7.4 In all cases, the Head of Internal Governance or his/her nominated deputy must be informed of and authorise all police requests.
16. **Data protection subject access request**

If any office or operator receives a data subject access request under the terms of the Data Protection Act 1998, these should be referred to the Head of Internal Governance or his/her nominated deputy who shall comply with the legal requirements of the request.

17. **Still digital prints (photographs)**

The CCTV equipment used by the NHSBSA has no facility to take or record still digital images.

18. **Dealing with incidents**

18.1 Physical security Incidents shall be dealt with according to locally agreed procedures (for example: damage to property and/or equipment, physical assault etc.).

18.2 Information security incidents (for example: theft of laptops, documents etc.), shall be dealt with according to the “Information Security Incident Reporting Procedure”.

18.3 Please note, in some instances a security incident can be both physical and information e.g. the theft of a laptop.

19. **Glossary**

19.1 Audit - periodic systematic examination of recorded data and records to review compliance with operational procedures and the Code of Practice.

19.2 Evaluation - independent assessment and appraisal of the CCTV scheme.

19.3 Monitor - routine and continuous checking and observation of compliance with operational procedures and the Code of Practice.

19.4 Owner - the organisation with overall responsibility for managing the scheme. The owner shall retain overall responsibility for the scheme and for carrying out certain requirements of the Code even when a contractor manages the scheme.

19.5 Operator - individuals responsible for operating the camera controls and other controlled area equipment.

19.6 Partnership - a local partnership can contain a range of local bodies e.g. The NHSBSA, Police, businesses, the Chamber of Commerce, and others may be involved.
19.7 Recorded data - includes, but is not limited to, material such as all forms of discs, DAT, compact disc, computer disk, digital print or film: media on which images are recorded and can be reconstituted later.

19.8 Scheme - the totality of the arrangements for closed circuit television in a locality, including, but not limited to, the technological system, staff, and the operational procedures.

19.9 System - the technological system in use in a CCTV scheme.

19.10 Disc - Digital disc.

20. Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Rev</th>
<th>Nature of Changes</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/07/11</td>
<td>A</td>
<td>New document.</td>
<td>I. Heywood</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Corporate cover sheet added.</td>
<td>N. Blevins</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Corporate header and footer added.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Equality statement added to section 1.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Legislation/guidance cross references added to section 2.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. Updated links and revised titles to internet documents.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. Section 3.2 Updated Benton Warehouse post code.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>8. Substantial rewrite and restructure of the document by I.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Heywood to meet the requirements of A Code of Practice for CCTV.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>9. Section 8.1.3 Information Governance website link added.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>10. Section 14.5 SHE Team contact details added for advice on health and safety.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>11. Corporate listing, tables, buleting and numbering standard applied.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>12. Section 20 (this section) added.</td>
<td></td>
</tr>
</tbody>
</table>