East Lindsey District Council CCTV Partnership

Code of Practice

for the operation of

Closed Circuit Television within East Lindsey

Section 1 Introduction and Objectives

1.1 Introduction

Closed Circuit Television (CCTV) systems have been introduced to Mablethorpe, Sutton on Sea, Alford, Louth, Skegness and Horncastle. This system, known as the East Lindsey District Council CCTV Partnership comprises a number of cameras installed at strategic locations. Most of the cameras are fully operational with pan, tilt and zoom facilities. Images will be monitored and recorded at the Control Room located at Skegness Police Station, Park Road, Skegness.

For the purposes of this document, the 'owner' of the system is East Lindsey District Council.

For the purposes of the Data Protection Act the 'data controller' is East Lindsey District Council.

The 'system manager' is East Lindsey District Council.

The East Lindsey District Council CCTV Partnership system has been notified to the Information Commissioner.

Details of key personnel, their responsibilities and contact points are shown at Appendix A to this Code.

1.2 Partnership statement in respect of The Human Rights Act 1998

1.2.1 The partnership recognises that public authorities and those organisations carrying of the functions of a public service nature are required to observe the obligations imposed by the Human Rights Act 1998, and consider that the use of CCTV in East Lindsey is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety.

1.2.2 This assessment is evidenced by an agreed 'operational requirement' document. Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for local authorities to provide closed circuit television coverage of any land within their area for the purposes of crime prevention or victim welfare and it is also considered a necessary initiative by East Lindsey District Council towards their duty under the Crime and Disorder Act 1998.

1.2.3 It is recognised that operation of the East Lindsey District Council CCTV Partnership System may be considered to infringe on the privacy of individuals. The partnership recognises that it is their responsibility to ensure that the scheme should always comply with all relevant legislation, to ensure its legality and legitimacy. The scheme will only be used as a proportional response to identified problems and be used only insofar as it is necessary in a democratic society, in the interests of national security, public safety, the economic well-being of the area, for the prevention and detection of crime or disorder, for the protection of

health and morals, or for the protection of the rights and freedoms of others.

1.2.4 The Codes of Practice and observance of the Operational Procedures contained in the manual shall ensure that evidence is secured, retained and made available as required to ensure there is absolute respect for everyone's right to a free trial.

1.2.5 The East Lindsey District Council CCTV Partnership System shall be operated with respect for all individuals, recognising the right to be free from inhuman or degrading treatment and avoiding discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

1.3 Objectives of the System

1.3.1 The objectives of the East Lindsey District Council CCTV Partnership System are as follows:

- To help reduce the fear of crime
- To help deter crime
- To help detect crime and provide evidential material for court proceedings
- To enhance community safety, assist in developing the economic well-being of the area
- To assist the Local Authority in its enforcement and regulatory functions within area
- To assist in Traffic Management
- To assist in supporting civil proceedings which will help detect crime

1.3.2 Service Level Agreements have been drawn up between East Lindsey District Council, Lincolnshire Police and the Town Councils of Alford, Horncastle, Louth, Mablethorpe and Sutton on Sea and Skegness.

1.4 Procedural Manual

This Code of Practice (hereafter referred to as 'the Code') is supplemented by a separate 'Procedural Manual' which offers instructions on all aspects of the day-to-day operation of the system. To ensure the purpose and principles of the East Lindsey CCTV system are realised, the procedural manual is based and expands upon the contents of this Code of Practice.

Section 2 Statement of Purpose and Principles

2.1 Purpose

The purpose of this document is to state the intention of the owners to support the objectives of East Lindsey District Council CCTV Partnership (hereinafter referred to as 'The Partnership') and to outline how it is intended to do so.

2.1.1 The 'Purpose' of the Partnership and the process adopted in determining the 'Reasons' for implementing the System are as previously defined in order to achieve the objectives detailed within Section 1.

2.2 General Principles of Operation

2.2.1 The system will be operated in accordance with all the requirements and the principles of the Human Rights Act 1998.

2.2.2 The operation of the System will also recognise the need for formal authorisation of any covert 'Directed' surveillance or crime-trend (hotspot) surveillance as required by the Regulation of Investigatory Powers Act 2000 and the Police Force policy.

2.2.3 The System will be operated in accordance with the Data Protection Act at all times.

2.2.4 The System will be operated fairly, within the law, and only for the purposes for which it was established and are identified within this Code, or which are subsequently agreed in accordance with this Code of Practice.

2.2.5 The System will be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and their home.

2.2.6 The public interest in the operation of the system will be recognised by ensuring the security and integrity of operational procedures.

2.2.7 Throughout this Code of Practice it is intended, as far as reasonably possible, to balance the objectives of the CCTV System with the need to safeguard the individual's rights. Every effort has been made throughout the Code to indicate that a formal structure has been put in place, including a complaints procedure, by which it can be identified that the System is not only accountable, but is seen to be accountable.

2.2.8 Participation in the System by any organisation, individual or authority assumes an agreement by all such participants to comply fully with this Code and to be accountable under the Code of Practice.

2.3 Copyright

Copyright and ownership of all material recorded by virtue of the System will remain with the data controller.

2.4 Cameras and Area Coverage

2.4.1 The areas covered by CCTV to which this Code of Practice refers are public areas within the East Lindsey geographic area.

2.4.2 From time to time transportable or mobile cameras may be temporarily sited within the area. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the CCTV Partnership and be governed by these Codes and Procedures.

2.4.3 Some of the cameras offer full colour, pan tilt and zoon (PTZ) capability, some of which may automatically switch to monochrome in low light conditions.

2.4.4 None of the cameras forming part of the System will be installed in a covert manner. Some cameras may be enclosed within 'All weather domes' for aesthetic or operational reasons, but the presence of all cameras will be identified by appropriate signs.

2.4.5 A map showing the number and location of all fixed cameras is attached at **Appendix 'A'** to these Codes.

2.5 Monitoring and Recording Facilities

2.5.1 A control room is located at Skegness Police station. The CCTV equipment has the capability of recording all cameras simultaneously throughout every 24 hour period.

2.5.2 No equipment, other than that housed within the main CCTV control room shall be capable of recording images from any of the cameras.

2.5.3 CCTV operators are able to record images, produce hard copies of recorded images, replay or copy any pre-recorded data at their discretion and in accordance with the Code of Practice. All viewing and recording equipment shall only be operated by trained and authorised users.

2.6 Human Resources

2.6.1 Unauthorised persons will not have access without an authorised member of staff being present.

2.6.2 The control room shall be staffed by specially selected and Security Industry Authority trained operators in accordance with the requirements of the Private Security Industry Act 2001.

2.6.3 All operators shall receive training relevant to their role in the requirements of the Human Rights Act 1998, Data Protection Act 1998,

Regulation of Investigatory Powers Act 2000 and the Codes of Practice and Procedures. Further training will be provided as necessary.

2.7 Processing and Handling of Recorded Material

2.7.1 All recorded material, recorded digitally or as a hard copy video print, will be processed and handled strictly in accordance with this Code of Practice and the Procedural Manual.

2.8 Operators Instructions

2.8.1 Technical instructions on the use of equipment housed within the control room are contained in a separate manual.

2.9 Changes to the Code or the Procedural Manual

2.9.1 Any major changes to either the Code of Practice or the Procedural Manual (i.e. such as will have a significant impact upon the Code of Practice or upon the operation of the system) will take place only after consultation with, and upon the agreement of all organisations with a participatory role in the operation of the system.

2.9.2 A minor change (i.e. such as may be required for clarification and will not have such a significant impact) may be agreed between the relevant partners.

Section 3 Privacy and Data Protection

3.1 Public Concern

3.1.1 Although the majority of the public at large may have become accustomed to 'being watched', those who do express concern do so mainly over matters pertaining to the processing of the information, (or data) i.e. what happens to the material that is obtained.

3.1.2 All personal data obtained by virtue of the System, shall be processed fairly and lawfully and, in particular, shall only be processed in the exercise of achieving the stated objectives of the System. In processing personal data there will be total respect for everyone's right to respect for his or her private and family life and their home.

3.1.3 The storage and security of the data will be strictly in accordance with the requirements of the Data Protection Act 1998 and additional locally agreed procedures.

3.2 Data Protection Legislation

3.2.1 The operation of the System has been notified to the Office of the Information Commissioner in accordance with current Data Protection legislation.

3.2.2 The 'data controller' for the System is East Lindsey District Council and day-to-day responsibility for the data will be devolved to the CCTV Manager.

3.2.3 All data will be processed in accordance with the principles of the Data Protection Act, 1998 which, in summarised form, includes, but is not limited to:

i) All personal data will be obtained and processed fairly and lawfully.

ii) Personal data will be held only for the purposes specified.

iii) Personal data will be used only for the purposes, and disclosed only to the people, shown within these Codes of Practice.

iv) Only personal data will be held which are adequate, relevant and not excessive in relation to the purpose for which the data are held.

v) Steps will be taken to ensure that personal data are accurate and where necessary kept up to date.

vi) Personal data will be held for no longer than is necessary.

vii) Individuals will be allowed access to information held about them and, where appropriate, permitted to correct or erase it.

viii) Procedures will be implemented to put in place security measures to prevent unauthorised or accidental access to, alteration, disclosure or loss and destruction of information.

3.3 Request for information (subject access)

3.3.1 Any request from an individual for the disclosure of personal data which he/she believes is recorded by virtue of the System will be directed in the first instance to the CCTV Manager.

3.3.2 The principles of Sections 7 and 8, 10 and 12 of the Data Protection Act 1998 (Rights of Data Subjects and Others) shall be followed in respect of every request; those Sections are reproduced as **Appendix 'B'** to these Codes.

3.3.3 If the request cannot be complied with without identifying another individual, permission from all parties must be considered (in the context of the degree of privacy they could reasonably anticipate from being in that location at that time) in accordance with the requirements of the legislation.

3.3.4 Any person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located. The appropriate 'Subject Access' request form is included in **Appendix 'C'**

3.4 Exemptions to the Provision of Information

In considering a request made under the provisions of Section 7 of the Data Protection Act 1998, reference may also be made to Section 29 of the Act which includes, but is not limited to, the following statement:

3.4.1 Personal data processed for any of the following purposes:-

i) the prevention or detection of crime
ii) the apprehension or prosecution of offenders

are exempt from the subject access provisions in any case 'to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection'.

3.5 Criminal Procedures and Investigations Act 1996

The Criminal Procedures and Investigations Act 1996 came into effect in April 1997 and introduced a statutory framework for the disclosure to defendants of material which the prosecution would not intend to use in the presentation of its own case, (known as unused material). An explanatory summary of the provisions of the Act is contained within the procedural manual, but disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on the data controller by Section 7 of the Data Protection Act 1998, (known as subject access).

Section 4 Accountability and Public Information

4.1 The Public

4.1.1 For reasons of security and confidentiality, access to the CCTV control room is restricted in accordance with this Code of Practice. However, in the interest of openness and accountability, anyone wishing to visit the room may be permitted to do so, subject to the approval of, and after making prior arrangements with, the Manager of the System.

4.1.2 Cameras will not be used to look into private residential property. Where the equipment permits it 'Privacy zones' will be programmed into the system as required, in order to ensure that the interior of any private residential property within range of the system is not surveyed by the cameras. If such 'zones' cannot be programmed the operators will be specifically trained in privacy issues.

4.1.3 A member of the public wishing to register a complaint with regard to any aspect of the System may do so by contacting the CCTV Manager. All complaints shall be dealt with in accordance with the complaints procedure, a copy of which may be obtained from East Lindsey CCTV Partnership. Any performance issues identified will be considered under the East Lindsey District Council's disciplinary procedures.

4.1.4 All CCTV staff are subject to regulations governing confidentiality and discipline. An individual who suffers damage or distress by reason of any contravention of this Code of Practice may be entitled to compensation.

4.2 System Owner

4.2.1 The Business Manager, Housing and Community Development, being the nominated representative of the system owners, will have unrestricted personal access to the CCTV control room and will be responsible for receiving regular and frequent reports from the Manager of the system.

4.2.2 East Lindsey District Council will nominate a committee with a specific responsibility for receiving and considering those reports.

4.2.3 Formal consultation will take place between the owners and the Managers of the system with regard to all aspects, including this Code of Practice and the Procedural Manual.

4.3 System Manager

4.3.1 The nominated manager will have day-to-day responsibility for the system as a whole.

4.3.2 The system will be subject to annual quarterly reports to Elected Members of East Lindsey District Council.

4.3.3 The system manager will ensure that every complaint is acknowledged in writing within five working days which will include advice to the complainant of the enquiry procedure to be undertaken. (A formal report will be forwarded to the nominee of the system giving details of all complaints).

4.3.4 Statistical and other relevant information, including any complaints made, will be included in the quarterly reports of East Lindsey District Council which are made publicly available.

4.4 Public Information

4.4.1 Code of Practice

A copy of this Code of Practice shall be published and a copy will be made available to anyone on request. Additional copies will be lodged at public libraries, Town Council Offices, Police Stations in Mablethorpe and Alford, East Lindsey District Council Offices and East Lindsey District Council's Website at www.e-lindsey.gov.uk

4.4.2 Signs

Signs will be placed in the locality of the cameras and at main entrance points to the district. The signs will indicate:

i) The presence of CCTV monitoring;
ii) The 'ownership' of the system;
iii) Contact telephone number of the 'data controller' of the system.

Section 5 Assessment of the System and Code of Practice

5.1 Evaluation

5.1.1 The System will periodically be evaluated to establish whether the purposes of the system are being complied with and whether objectives are being achieved. The format of the evaluation shall comply with that laid down by the Home Office Statistics and Research Directorate in the Home Office Bidding Guidelines and be based on assessment of The Inputs, The Outputs, The Process and the Impact of the scheme.

Objectives

i) An assessment of the impact upon crime: This assessment shall include not only the immediate area covered by the cameras but the wider town area, the Police Divisional and regional areas and national trends.

ii) An assessment of the incidents monitored by the system.

iii) An assessment of the impact on town centre business.

iv) An assessment of neighbouring areas without CCTV.

v) The views and opinions of the public.

vi) The operation of the Code of Practice.

vii) Purposes for which the system was established are still relevant.

viii) Cost effectiveness

5.1.2 The results of the evaluation will be available to Members and Officers of East Lindsey District Council and will be used to review and develop any alterations to the specified purpose and objectives of the scheme as well as the functioning, management and operation of the system.

5.1.3 It is intended that evaluations should take place every year.

5.2 Monitoring

5.2.1 The System Manager will accept day-to-day responsibility for the monitoring, operation and evaluation of the system and the implementation of this Code of Practice.

5.2.2 The System Manager shall also be responsible for maintaining full management information as to the incidents dealt with by the control room, for use in the management of the system and in future evaluations.

5.3 Audit

5.3.1 Internal Audit will be responsible for regularly auditing the operation of the system and the compliance with this Code of Practice. Audits, which may be in the form of irregular spot checks, will include examination of the control room records, digital recording histories and the content of recorded material.

5.4 Inspection

5.4.1 A body of individuals who have no direct contact or relationship with the operation of the system may be appointed to be responsible for inspecting the operation of the system.

5.4.2 Inspections should take place at least six times per calendar year by no more than two people at any one time. The inspectors will be permitted access to the CCTV control room, without prior notice and to the records held therein at any time, provided their presence does not disrupt the operational functioning of the room. Their findings will be reported to the Auditor and their visit recorded in the CCTV control room.

5.4.3 Inspections will be required to sign a declaration of confidentiality (see **Appendix 'D'**)

Section 6 Human Resources

6.1 Staffing of the Control Room and those responsible for the operation of the system

6.1.1 The CCTV Control Room will be staffed in accordance with the procedural manual. Equipment associated with the System will only be operated by authorised personnel who will have been properly trained in its use and all control room procedures.

6.1.2 Every person involved in the management and operation of the system will be personally issued with a copy of both the Code of Practice and the Procedural Manual, will be required to sign a confirmation that they fully understand the obligations adherence to these documents places upon them and that any breach will be considered as a disciplinary offence. They will be fully conversant with the contents of both documents, which may be updated from time to time, and which he/she will be expected to comply with as far as is reasonably practicable at all times.

6.1.3 Arrangement may be made for a Police Liaison Officer to be present in the Control Room at any time, subject to locally agreed protocols. Any such person must also be conversant with this Code of Practice and associated Procedural Manual.

6.1.4 All personnel involved with the system shall receive training from time to time in respect of all legislation appropriate to their role as required by Security Industry Authority Guidelines.

6.2 Discipline

6.2.1 Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with the System to which they refer, will be subject to the East Lindsey District Council discipline code. Any breach of this Code of Practice or of any aspect of confidentiality will be dealt with in accordance with those discipline rules.

6.2.2 The System Manager will accept primary responsibility for ensuring there is no breach of security and that the Code of Practice is complied with. He/she has day-to-day responsibility for the management of the room and for enforcing the discipline rules. Non-compliance with this Code of Practice by any person will be considered a severe breach of discipline and dealt with accordingly including, if appropriate, the instigation of criminal proceedings.

6.3 Declaration of Confidentiality

Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with the System to which they refer, will be required to sign a declaration of confidentiality (see example at **Appendix 'D'**, see also Section 8 concerning access to the control room by others).

Section 7 Control and Operation of Cameras

7.1 Guiding Principles

7.1.1 Any person operating the cameras will act with utmost probity at all times.

7.1.2 The cameras, control equipment, recording and reviewing equipment shall at all times only be operated by persons who have been trained in their use and the legislative implications of their use.

7.1.3 Every use of the cameras will accord with the purposes and key objectives of the system and shall be in accordance with this Code of Practice.

7.1.4 Cameras will not be used to look into private residential property. 'Privacy zones' shall be programmed into the system (whenever practically possible) in order to ensure that the interior of any private residential property within range of the system is not surveyed by the cameras.

7.1.5 Camera operators will be mindful of exercising prejudices which may lead to complaints of the system being used for purposes other than those for which it is intended. The operators may be required to justify their interest in, or recording of, any particular individual, group of individuals or property at any time by virtue of the audit of the system or by the System Manager.

7.2 Primary Control

7.2.1 Only those trained and authorised members of staff with responsibility for using the CCTV equipment will have access to the operating controls.

7.3 Secondary Control

7.3.1 No secondary control or recording facilities are installed.

7.4 Operation of the System by the Police

7.4.1 Under extreme circumstances the Police may make a request to assume direction of the System to which this Code of Practice applies. Only requests made on the written authority of a Police Officer not below the rank of Superintendent will be considered. Any such request will only be accommodated on the personal written authority of the CCTV Manager.

7.4.2 In the event of such a request being permitted, the Control Room will continue to be staffed, and equipment operated by, only those personnel who are authorised to do so, and who fall within the terms of Sections 6 and 7 of this Code, who will then operate under the direction of the Police Officer designated in the written authority.

7.4.3 In very extreme circumstances a request may be made for the Police to take control of the System in its entirety, including the staffing of the control room and personal control of all associated equipment, to be exclusion of all representatives of the System owners. Any such request should be made to the System Manager in the first instance, who will consult personally with the most senior officer of the System owners (or designed deputy of equal standing). A request for total exclusive control must be made in writing by a Police Officer not below the rank of Assistant Chief Constable or person of equal standing.

7.5 Maintenance of the System

7.5.1 To ensure compliance with the Information Commissioners Code of Practice and that images recorded continue to be of appropriate evidential quality the System shall be maintained in accordance with the requirements of the Procedural Manual under a maintenance agreement.

7.5.2 The maintenance agreement will make provision for regular/periodic service checks on the equipment which will include cleaning of any all-weather domes or housings, checks on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality.

7.5.3 The maintenance will also include regular periodic overhaul of all the equipment and replacement of equipment which is reaching the end of its serviceable life.

7.5.4 The maintenance agreement will also provide for 'emergency' attendance by a specialist CCTV engineer on site to rectify any loss or severe degradation of image or camera control.

7.5.5 The maintenance agreement will define the maximum periods of time permitted for attendance by the engineer and for rectification of the problem depending upon the severity of the event and the operational requirements of that element of the system.

7.5.6 It is the responsibility of the System Manager to ensure appropriate records are maintained in respect of the functioning of the cameras and the response of the maintenance organisation.

Section 8 Access to, and Security of, Control Room and Associated Equipment

8.1 Authorised Access

8.1.1 Only trained and authorised personnel will operate any of the equipment located within the CCTV Control Room (or equipment associated with the CCTV System).

8.2 Public Access

8.2.1 Public access to the Control Room will be prohibited. Except for with lawful, proper and sufficient reason and only then with the personal authority of the CCTV Manager. Any such visits will be conducted and recorded in accordance with the Procedural Manual.

8.3 Authorised Visits

8.3.1 Visits by inspectors or auditors do not fall into the scope of the above paragraph and may take place at any time, without prior warning. No more than two inspectors or auditors will visit at any one time. Inspectors or Auditors will not influence the operation of any part of the system during their visit. The visit will be suspended in the event of it being operationally inconvenient. Any such visit should be recorded in the same way as that described above.

8.4 Declaration of Confidentiality

8.4.1 Regardless of their status, all visitors to the CCTV Control Room will be required to sign the visitors book and a declaration of confidentiality.

8.5 Security

8.5.1 Authorised personnel will normally be present at all time when the equipment is in use. If the monitoring facility is to be left unattended for any reason it will be secured. In the event of the Control Room having to be evacuated for safety or security reasons, the provisions of the Procedural Manual will be complied with. Proximity reader type locks are in place at the Control Room door.

8.5.2 The Control Room will at all times be secured by 'Magnetic Locks' operated by the CCTV operator.

8.5.3 A fixed view camera is located within the Control Room to monitor the entry and exit of people to the Control Room.

Section 9 Management of Recorded Material

9.1 Guiding Principles

9.1.1 For the purposes of this Code 'recorded material' means any material recorded by, or as the result of, technical equipment which forms part of the System, but specifically includes images recorded digitally, or on videotape or by way of video copying, including video prints and CD ROMs.

9.1.2 Every digital recording obtained by using the System has the potential of containing material that has to be admitted in evidence at some point during its life span.

9.1.3 Members of the community must have total confidence that information recorded about their ordinary every day activities by virtue of the System, will be treated with due regard to their individual right to respect for their private and family life.

9.1.4 It is therefore of the utmost importance that irrespective of the means or format (e.g. paper copy, video tape, digital tape, CD, or any form of electronic processing and storage) of the images obtained from the system, they are treated strictly in accordance with this Code of Practice and the Procedural Manual from the moment they are received by the Control Room until final destruction. Every movement and usage will be meticulously recorded.

9.1.5 Access to and the use of recorded material will be strictly for the purposes defined in this Code of Practice only.

9.1.6 Recorded material will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment.

9.2 National standard for the release of data to a third party

9.2.1 Every request for the release of personal data generated by this CCTV System will be channelled through the System Manager. The System Manager will ensure the principles contained within **Appendix 'E'** to this Code of Practice are followed at all times.

9.2.2 In complying with the national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's right to privacy and to give effect to the following principles:

- Recorded material shall be processed lawfully and fairly and used only for the purposes defined in this Code of Practice;
- Access to recorded material will only take place in accordance with the standards outlined in **Appendix 'E'** to this Code of Practice;
- The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

9.2.3 Members of the Police service or other agency having a statutory authority to investigate and/or prosecute offences may, subject to compliance with **Appendix 'E'**, release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses. Under such circumstances, full details will be recorded in accordance with the Procedural Manual.

9.2.4 If material is to be shown to witnesses, including Police Officers, for the purpose of obtaining identification evidence, it must be shown in accordance with **Appendix 'E'** and the Procedural Manual.

9.2.5 It may be beneficial to make use of 'real' video footage for the training and education of those involved in the operation and management of CCTV systems, and for those involved in the investigation, prevention and detection of crime. Any material recorded by virtue of this CCTV system will only be used for such bona fide training and education purposes. Recorded material will not be released for commercial or entertainment purposes.

9.3 Blank

9.4 Image - Retention

9.4.1 Recorded images will be retained for a period of at least 28 days.

9.5 Blank

9.6 Recording Policy

9.6.1 Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24 hour period through digital multiplexers onto digital hard disks. The number of frames recorded on a digital system will be such that the time between successive frames once played back in time lapse mode shall not exceed 2 seconds.

9.6.2 Images from selected cameras will be recorded in real time at the discretion of the CCTV operators or as directed by the System Manager.

9.7 Evidential CD Roms

9.7.1 In the event of a CD Rom being required for evidential purposes the procedures outlined in the Procedural Manual will be strictly complied with.

Section 10 Video Prints

10.1 Guiding Principles

10.1.1 A video print is a copy of an image or images which already exist on computer disc. Such prints are equally within the definitions of 'data' and recorded material.

10.1.2 Video prints will not be taken as a matter of routine. Each time a print is made it must be capable of justification by the originator who will be responsible for recording the full circumstances under which the print is taken in accordance with the Procedural Manual.

10.1.3 Video prints contain data and will therefore only be released under the terms of **Appendix 'E'** to this Code of Practice, 'Release of data to third parties'. If prints are released to the media (in compliance with **Appendix 'E'**), in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with the Procedural Manual.

10.1.4 A record will be maintained of all video print productions in accordance with the Procedural Manual. The recorded details will include: a sequential number, the date, time and location of the incident, date and time of the production of the print and the identity of the person requesting the print (if relevant) and the purpose for which the print was taken.

10.1.5 The records of the video prints taken will be subject to audit In common with all other records in the system.

Section 8

(1) The Secretary of State may by regulations provide that, in such cases as may be prescribed, a request for information under any provision of subsection (1) of section 7 is to be treated as extending also to information under other provisions of that subsection.

(2) The obligation imposed by section 7(1)(c)(i) must be complied with by supplying the data subject with a copy of the information in permanent form unless:

(a) the supply of such a copy is not possible or would involve disproportionate effort, or

(b) the data subject agrees otherwise;

(c) and where any of the information referred to in section 7(1)(c)(i) is expressed in terms which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.

(3) Where a data controller has previously complied with a request made under section 7 by an individual, the data controller is not obliged to comply with a subsequent identical or similar request under that section by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

(4) In determining for the purposes of subsection (3) whether requests under section 7 are made at reasonable intervals, regard shall be had to the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.

(5) Section 7(1)(d) is not to be regarded as requiring the provision of information as to the logic involved in decision-taking if, and to the extent that, the information constitutes a trade secret.

(6) The information to be supplied pursuant to request under section 7 must be supplied by reference to the data in question at the time when the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.

(7) For the purposes of section 7(4) and (5) another individual can be identified from the information being disclosed if he/she can be identified from that information, or from that and any other information which, in the reasonable belief of the data controller, is likely to be in, or to come into, the possession of the data subject making the request.