



# **NEWARK and SHERWOOD CCTV SCHEME**

**Code of Practice**  
in respect of the operation of  
**Closed Circuit Television**  
**AMENDED**

## Contents

Index	Page 1
Acknowledgement	Page 2
Certificate of Agreement	Page 3
Introduction and Objectives	Section 1
Statement of Purpose and Principles	Section 2
Privacy and Data Protection	Section 3
Accountability and Public Information	Section 4
Assessment of the System and the Code of Practice	Section 5
Human Resources	Section 6
Control and Operation of the Cameras	Section 7
Access to, and Security of, Monitoring Room and/or Associated Equipment	Section 8
Management of Recorded Material	Section 9
Intrusive / Directed surveillance	Section 10
Mobile CCTV	Section 11
<b>Appendices</b>	
Key Personnel and their Responsibilities	Appendix A
Extracts from the Data Protection Act, 1998	Appendix B
National Standard for the Release of Data to Third Parties	Appendix C
Restricted Access Notice	Appendix D
Declaration of Confidentiality (Operator/Manager)	Appendix E
Declaration of Confidentiality (Inspector)	Appendix F
Subject Access Request Form	Appendix G
CCTV equipment booking out form	Appendix H
Mobile CCTV Advisory / Loan Form	Appendix I

## **Acknowledgement**

This Framework Code of Practice is based upon a draft code prepared by:

The Standards Committee of the CCTV User Group

PO Box 6023

Leighton Buzzard

Bedfordshire

LU7 0YU

# Code of Practice

in respect of the operation of CCTV in

NEWARK, SOUTHWELL, CLIPSTONE & OLLERTON TOWN CENTRES

An operational partnership agreement between

NEWARK AND SHERWOOD DISTRICT COUNCIL

and

NOTTINGHAMSHIRE POLICE

## ***Certificate of Agreement***

*The content of both this Code of Practice and the Procedural Manual are hereby approved in respect of the NEWARK AND SHERWOOD Closed Circuit Television System and, as far as reasonably practicable, will be complied with by all who are involved in the management and operation of the System.*

Signed for and on behalf of:

NEWARK AND SHERWOOD DISTRICT COUNCIL

Signature: ..... Name: Andrew Muter

Position held: CHIEF EXECUTIVE

Dated the ..... day of ..... 2009

Signed for and on behalf of NOTTINGHAMSHIRE POLICE

Signature: ..... Name: .....

Position held: CHIEF SUPERINTENDENT

Dated the ..... day of ..... 2009

## Section 1

### Introduction and Objectives

#### I Introduction

A digital monitored camera system known commonly as Closed Circuit Television (CCTV), operates in the areas of Newark on Trent, Southwell and other areas within the District of Newark & Sherwood. The system, which is known as the 'Newark and Sherwood CCTV System', comprises of a number of cameras installed at strategic locations, which includes cameras that are fully operational with pan, tilt and zoom facilities and some which are fixed cameras. Secondary monitoring facilities are located at other locations (eg. Police HQ control room) but there are no recording or control facilities at any location other than the monitoring room. In addition a mobile/relocatable system is operated (see Section 11) as well as an I.P. (Broadband Internet) System.

The Newark CCTV System has evolved from the formation of a partnership between Newark and Sherwood District Council, the Community and Nottinghamshire Police. For the purposes of this document, the 'owner' of the system is Newark and Sherwood District Council and the 'manager' and therefore 'data controller'<sup>(1)</sup> is by delegation the Corporate Manager of Risk & Resilience. Details of key personnel, their responsibilities and contact points are shown at Appendix A to this Code.

#### II Objectives of the System

- a) The objectives of the system are:
- To help reduce the fear of crime.
  - To help deter crime and detect crime.
  - To assist in the overall management of Newark and Southwell town centres.
  - To enhance community safety, boost the economy and encourage greater use of the town centre/shopping areas, etc.
  - To assist the Local Authority in its enforcement and regulatory functions within the town centre.
  - To assist with traffic management.
  - To assist in supporting civil proceedings help detect crime, and
  - To assist in the safety and well-being of the public.
- b) Within this broad outline, the Local Police Commander, in partnership with the Chief Executive will, where necessary, also draw up, and publish specific key objectives (which will be reviewed annually) based on the Newark and Sherwood Crime and Disorder Partnership.

#### III Procedural Manual

This Code of Practice (hereafter referred to as 'the Code') will be supplemented by a separate Procedural Manual/Assignment Instructions which offer instructions on all aspects of the operation of the system. To ensure the purpose and principles (see Section 2) of the CCTV system are realised, the Manual is based upon the contents of this Code of Practice.

Notes:

- (1) *The **data controller** is the person or organisation who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal data are, or are to be, processed. (In most cases the data controller is likely to be the scheme owner or manager).*

## Section 2

### Statement of Purpose and Principles

#### I Purpose

The purpose of this document is to state the intention of both the owner and the manager, on behalf of the partnership as a whole and as far as is reasonably practicable, to support the objectives of the Newark and Sherwood CCTV System (hereafter referred to as 'the System') and to outline how it is intended to do so.

#### II General Principles

- a) The System will be operated fairly, within the law, and only for the purposes for which it was established or which are subsequently agreed in accordance with this Code of Practice.
- b) 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 and with specific regard to the Data Protection Act 1998 and the Human Rights Act 2000.
- c) The public interest in the operation of the System will be recognised by ensuring the security and integrity of operational procedures.
- d) Throughout this Code of Practice it is intended, as far as is reasonably practicable, to offer a balance between the objectives of the CCTV System and the need to safeguard the individual's right to privacy. Throughout the Code every effort has been made to indicate that a formal structure has been put in place (including a complaints procedure) by which it should be identified that the System is not only accountable, but is seen to be accountable.
- e) Participation in the System by any local 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.

#### III Copyright

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

#### IV Cameras and Area Coverage

The areas covered by CCTV to which this Code of Practice refers are Newark, Southwell and Ollerton town centres, areas in Balderton and Clipstone, the Newark lorry park/car parks and the Riverside area, Kelham Hall and Car Parks. From time to time transportable or mobile cameras may be temporarily or long term 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 System.

The majority of the cameras, offer full colour, pan tilt and zoom (PTZ) capability, some of which may automatically switch to monochrome in low light conditions. None of the cameras forming part of the System will be installed in a covert manner<sup>(1)</sup>.

Notes:

- (1) *The installation of a CCTV camera is considered to be overt unless it is installed in a manner whereby its presence is deliberately intended to be concealed from the view of any person likely to be within the field of view of that camera.*

*Cameras which may be placed in domes or covered to reduce the likelihood of assessing their field of view, or to protect them from weather or damage, would not be regarded as covert provided that appropriate signs indicating the use of such cameras are displayed in the vicinity.*

## **V Monitoring and Recording Facilities**

- a) A staffed monitoring room is located at the Council Offices. The CCTV equipment has the capability of recording all cameras simultaneously throughout every 24 hour period.
- b) Secondary monitoring equipment is located in Newark Police Station and Mansfield Police HQ Control Room. However the Police control rooms have no capability to record images from any of the cameras (2).
- c) All fixed camera images are recorded in real time, mobile camera images may be recorded at less than full frame rate. CCTV operators can produce hard copies of recorded images, replay or copy any pre-recorded data in accordance with the Code of Practice.

## **VI Human Resources**

Authorised persons will normally be present whenever the monitoring equipment is in use.

## **VII Processing and Handling of Recorded Material**

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

## **VIII Operators Instructions**

Technical instructions on the use of equipment housed within the monitoring room are contained in a separate manual provided by the equipment suppliers.

## **IX Changes to the Code or the Procedural Manual**

- a) Any major changes to either the Code 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 all relevant interested groups, and upon the agreement of all organisations with a participatory role in the operation of the system.
- b) 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 manager and the owner of the System.

*Notes:*

- (2) *It is acknowledged that many CCTV Systems are operated on a 'part-time' basis or without the benefit of a staffed monitoring room. In such cases reference to 'monitoring rooms' throughout this Code should be applied to existing monitoring and recording facilities as appropriate.*

*It is also recognised that, in the interest of security and operator safety, some CCTV System owners do not wish the precise location of the relevant monitoring room to be included within the text of a Code of Practice.*

## Section 3

# Privacy and Data Protection

### I Public Concern

- a) 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.

### II Data Protection Legislation

- a) Although most CCTV Systems were not specifically included under the terms of the 1984 Act, most, if not all Systems come within the terms of the Data Protection Act 1998. The implementation date of the new Act was 24 October 1998. Any processing which commences after that date needs to be fully compliant with the Act.
- b) The Newark and Sherwood CCTV System is registered with the office of the Data Protection Commissioner; with the Corporate Manager of Risk and Resilience being nominated as the data controller.
- c) All data however 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 this Code of Practice.
  - iv) Only personal data will be held which is adequate, relevant and not excessive in relation to the purpose for which the data is held.
  - v) Steps will be taken to ensure that personal data is 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, where appropriate, access to information held about them and where appropriate, permitted to correct or erase it. (See III below)
  - 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.

### III Request for information (subject access)

- a) 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 to the System manager (or data controller).
- b) The principles of Sections 7 and 8 of the Data Protection Act 1998 (Rights of Data Subjects and Others) should be followed in respect of every request, those Sections are reproduced as Appendix B to these Codes.
- c) Access requests can only be made using the proforma as found in Appendix G.

#### **IV 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:

- a) Personal data processed for either of the following purposes:
  - i) The prevention or detection of crime;
  - ii) The apprehension or prosecution of offenders

is 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'.

**Note: Each and every application will be assessed on its own merits and general 'blanket exemptions' will not be applied.**

#### **V 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

#### I The Public

- a) For reasons of security and confidentiality, access to the CCTV monitoring room is restricted in accordance with this Code of Practice. However, in the interest of openness and accountability, anyone wishing to arrange an official visit to the room may be permitted to do so, subject to the approval of, and after making prior arrangements with, the manager of the System.
- b) Cameras will not be used to look into private residential property. 'Privacy zones' are 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.
- c) A member of the public wishing to register a complaint with regard to any aspect of the Newark CCTV System may do so by contacting The Corporate Manager of Risk and Resilience on 01636 650000. Any such complaint will be dealt with in accordance with existing discipline rules and regulations to which all members of the partnership, including the CCTV operators, are subject. An individual who suffers damage or distress by reason of any clear contravention of this Code of Practice, may be entitled to compensation from the System owner or operator.

#### II (System owner)

- a) Newark and Sherwood District Council, named at Appendix A, being the nominated representative/s of the System owners, will have unrestricted personal access to the CCTV monitoring room and will be responsible for receiving regular and frequent reports from the manager of the System.
- b) Newark and Sherwood District Council may nominate a committee with a specific responsibility for receiving and considering those reports.
- c) 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.

#### III (System manager) [or data controller]

- a) The nominated manager named at Appendix A will have day-to-day responsibility for the System as a whole.
- b) The System manager will ensure that every complaint is acknowledged in writing within seven working days which will include advice to the complainant of the enquiry procedure to be undertaken. A formal six monthly report will be forwarded to the nominee of the System owner named at Appendix A, giving details of all complaints and the outcome of relevant enquiries.
- c) Statistical and other relevant information, including any complaints made, will be included in the Annual Report of the Newark CCTV Scheme which will be made publicly available.

#### IV Public Information

- a) Code of Practice: A copy of this Code of Practice will be made available to anyone requesting it. A copy is available online at <http://www.newark-sherwooddc.gov.uk/pp/gold/viewGold.asp?IDType=Page&ID=6562>. Additional copies will be lodged at public libraries, Nottinghamshire Police Station at Newark, offices of Newark and Sherwood District Council at Kelham Hall and Newark Town Hall cash office.
- b) Annual Report: A copy of the annual report will also be made available to anyone requesting it. Additional copies will be lodged at public libraries, Newark Police Station, offices of Newark and Sherwood District Council at Kelham Hall and Newark Town Hall cash office.
- c) CCTV Liaison Group: This group comprises of the District Council, the Police, Nottinghamshire County Council, Newark Town Council, Southwell Town Council and representatives from residents and business owners within Newark and Sherwood District area. Its remit is to monitor and make recommendations re performance of the system and to review the response to complaints and access requests.
- c) Signs: Signs will be placed in the locality of the cameras and at main entrance points to the relevant areas, eg. Railway and Bus stations. The signs will indicate:
  - i) The presence of CCTV monitoring and the purpose of the System.
  - ii) The 'ownership' of the System, i.e. Newark and Sherwood District Council, and
  - iii) Contact telephone number of the 'data controller' of the System.

## Section 5

### Assessment of the System and Code of Practice

#### I) Monitoring

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.

#### II) Inspection

- a) A body of individuals (lay inspectors) who have no direct contact with the System will be responsible for inspecting the operation of the System.
- b) Inspections should take place at least once per calendar year, including formal reviews by no more than two people at any one time. The Inspectors will be permitted access to the CCTV monitoring 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 and they are accompanied by an authorised person. Their findings will be reported to the System manager and made available to the relevant committee of the District Council and their visit recorded in the CCTV monitoring room.
- c) Inspectors will be required to sign a declaration of confidentiality (see Appendix F).

## Section 6

### Human Resources

#### I Staffing of the Monitoring Room

- a) The CCTV Monitoring Room will be staffed in accordance with the Procedural Manual. Equipment associated with the CCTV System will only be operated by authorised personnel who will have been properly trained in its use and all monitoring room procedures. Each operator will be personally issued with a copy of both the Code of Practice and the Procedural Manual/Assignment instructions. They will be fully conversant with the contents of such 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.

Each operator will be fully SIA licensed (CCTV Public Space Surveillance Operations) and whereby an operator is in training they will be monitored by a fully licensed operator.

- b) Arrangement may be made for a police liaison officer to be present in the monitoring room at certain times, subject to locally agreed protocols. Any such person must also be conversant with this Code of Practice and associated Procedural Manual/Assignment Instructions.

#### II Discipline

- a) Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with the CCTV System to which they refer, will be subject to Newark CCTV Scheme 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.
- b) 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.

#### III Declaration of Confidentiality

Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with the CCTV System to which it refers, will be required to sign a declaration of confidentiality. (See example at Appendix E, see also Section 8 concerning access to the monitoring room by others).

## Section 7

# Control and Operation of the Cameras

### I Guiding Principles

- a) Any person operating the cameras will act with utmost probity at all times and with regard to the requirements of the Data Protection Act 1998 and the Human Rights Act of 2000.
- b) Every use of the cameras will accord with the purposes and key objectives of the System and shall be in compliance with this Code of Practice.
- c) Cameras will not be used to look into private residential property. '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.
- d) 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.
- e) The System manager, where appropriate to do so, may invite residents from properties within the CCTV monitored area to the Control Room to enhance their confidence of privacy etc.

### II Primary Control

Only those authorised members of staff with responsibility for using the CCTV equipment will have access to the operating controls, those operators have primary control at all times.

### III Secondary Control

Secondary (*slave*) monitoring will be provided at Newark Police Station, Mansfield Police HQ Control and at times of exceptional need within Kelham Hall.

### IV Operation of the System by the Police

- a) Under extreme circumstances the Police may make a request to assume control of the CCTV System to which this Code of Practice applies. Only requests made on the written authority of a police officer not below the rank of Inspector will be considered. Any such request will only be accommodated on the personal written authority of the most senior representative available of the System owners, (*or designated deputy of equal standing*). This may be faxed to avoid delay.
- b) In the event of such a request being permitted, the Monitoring 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 Six and Seven of this Code.
- c) In very extreme circumstances a request may be made for the Police to take total control of the System in its entirety, including the staffing of the monitoring room and personal control of all associated equipment; to the exclusion of all representatives of the System owners. Any such request will only be considered personally by the most senior officer of the System owners (*or designated 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.

## Section 8

### Access to, and Security of, Monitoring Room and/or Associated Equipment

#### I **Authorised Access**

Only authorised personnel will operate any of the equipment located within the CCTV monitoring room or equipment associated with the CCTV System.

#### II **Public Access**

Public access to the monitoring and recording facility will be prohibited except for lawful, proper and sufficient reasons and only then with the personal authority of the System manager. Any such visits will be conducted and recorded in accordance with the Procedural Manual.

#### III **Authorised Visits**

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 but with the presence of the manager or other authorised person. 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.

#### IV **Declaration of Confidentiality**

Regardless of their status, all visitors to the CCTV monitoring room, including Inspectors and Auditors, will be required to sign the visitors log and a declaration of confidentiality.

#### V **Security**

Authorised personnel will normally be present at all times 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 monitoring room having to be evacuated for safety or security reasons, the provisions of the Procedural Manual will be complied with.

## Section 9

# Management of Recorded Material

### I Guiding Principles

- a) 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 Newark and Sherwood Closed Circuit Television System, but specifically includes images recorded digitally, or on videotape or by way of video copying, including video prints.
- b) Every video recording used in conjunction with the Newark and Sherwood CCTV System has the potential of containing material that has to be admitted in evidence at some point during its life span.
- c) 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.
- d) It is therefore of the utmost importance that every means of video recording is treated strictly in accordance with this Code of Practice and the Procedural Manual from the moment it is delivered to the monitoring room until its final destruction. Every movement and usage will be meticulously recorded.
- e) Access to, and the use of, recorded material will be strictly for the purposes defined in this Code of Practice only.
- f) Recorded material will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment, unless in the interest of crime prevention and authorised by a Police Inspector and the 'Data Controller', and not for financial gain.

### II National Standard for the Release of Data to a Third Party

- a) 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 C to this Code of Practice are followed at all times.
- b) 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 rights to privacy and to give effect to the following principles:
  - i) Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in this Code of Practice.
  - ii) Access to recorded material will only take place in accordance with the standards outlined in Appendix C and this Code of Practice.
  - iii) The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.
- c) Members of the police service or other agency having a statutory authority to investigate and/or prosecute offences may, subject to compliance with Appendix C, 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.

*Note: Release to the media of recorded information, in whatever format, which may be part of a current investigation would be covered by the Police and Criminal Evidence Act, 1984. Any such disclosure should only be made after due consideration of the likely impact on a criminal trial. Full details of any media coverage must be recorded and brought to the attention of both the prosecutor and the defence.*

- d) 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 C and the Procedural Manual.

### **III Digital Image recording**

- a) All Images are recorded digitally from camera source onto a Synectics Digital CCTV solution Raid 6 Hard drive or stand alone PC Hard drive. The images are recorded at 25 Frames per Second (full motion) and stored for a minimum 28 days before being deleted/reused.
- b) Images will only be retained longer than 28 days if they are expected to be used or used as evidence in an investigation or its case history.
- c) Evidence will normally be issued to the prosecuting authorities on two DVD's, both copies are considered to be primary evidence but one copy will be labelled as the Blue Working copy and the other will be labelled as the Red Master copy. Both copies will be issued to the Police on request and no further incident data will be held in CCTV after 28 days.
- d) In circumstances where a large amount of data is required a USB hard drive or USB stick may be utilised to hold large amounts of raw evidential data. Media player software is included in the process so that the data can be accessed by the Police using their own IT equipment. USB Hard Drives and/or other mass storage devices must be supplied by the Police.
- e) All production and movement of evidential material is recorded both on the Synectics digital recording system management interface and on the CCTV control room paperless office management system, Video Technology Advisory Service (VTAS).

### **IV Major Crime and Requests for Confiscation of System Hard Drives**

- a) The Digital Recording system has been designed and built with the express intention of providing evidential material to the Police and prosecuting authorities. The system stores evidential data for 28 days, the stored data can be downloaded on request onto various forms of storage media for investigation and production in court as prime evidence.
- b) The digital recording mechanism is built into a complex server unit, housed within the ICT Restricted Access server room. The Synergy Primary Storage Node (PSN) is a Raid 6 storage array with dual hot swap PSU's and dual network interface cards.
- c) The PSN units cannot be removed without the entire system being shut down, this can only be actioned by Synectics engineers. Once removed the system cannot be operated until the PSN units are replaced or replacement PSN units are built to the exact same specifications.
- d) If the PSN Units are removed they cannot be viewed unless placed into an identical system, which has been configured in the same way. Attempting to access the data on PSN units in a system which is not identically configured may result in the loss of some or all of the data.
- e) It is estimated that the entire CCTV data bank can be downloaded onto 28 X 1TB Hard Drives on request. This process is quicker than the same process using VHS Tapes but will still take several days. Standard USB Hard drives can be purchased at any electronics shop, these will not be supplied by the Council.

**V Special Warning to Investigating Officers on Requests to Remove PSN Units**

- a) Removal of PSN units as part of any investigation, no matter how important it is deemed, will prevent any further recording of CCTV cameras. This will result in the loss of evidence from many other minor and major incidents until the PSN units are replaced.
- b) Immediate complaints and requests for prosecuting action will be taken if any damage is caused to the Digital Recording system as a result of unwarranted access to the recording system or the removal of PSN units.
- c) Justification and compensation for the actions of Investigating Officers will be sought through the Nottinghamshire Chief Constable, where the removal of PSN units has occurred and CCTV operations across the Newark & Sherwood District Council/ B Division area have ceased or costs relating to the removal of PSN units have occurred.
- d) In exceptional circumstances recording of further evidence can be stopped to preserve already recorded data from being erased, until it can be down loaded onto other media. However the System itself will still be operational.
- e) When considering PSN removal, officers should consider that data may provide evidence for investigation and prosecution action, removal of parts of the System itself will not.

**VI Video Tapes - Provision & Quality (Older Storage System No Longer in Use and Phasing Out)**

- a) Tapes will be used a maximum of 15 times before being destroyed.
- b) After each use, tapes are held for a 28 day retention period, all non evidential tapes are then degaussed before reuse or destroyed after the maximum use has been reached.
- c) Any tapes still in use are evidential tapes which must be retained until the offender's case deadline or sentence has expired.
- d) Tapes may still be used for older mobile camera systems and the CCTV Van recorders only.

## Section 10

### Intrusive/Directed Surveillances

- I** There will be occasions when the Police need to, or plan to observe people, vehicles, premises or people entering and leaving premises as part of an investigation. The Human Rights Act 1998, aims to protect the individual's right to privacy. The RIPA Act 2000 (Regulation of Investigatory Powers Act) has been introduced to enable the Police to incorporate legislation and to formalize surveillance procedures in line with provisions of the Human Rights Act.
- II** When assisting the Police, there are two categories of surveillance:
- a) Directed surveillance - surveillance undertaken for a specific investigation or operation, in a manner likely to obtain private information.
  - b) Intrusive surveillance - surveillance taking place in or into private premises or a private vehicle, in a manner intended to obtain private information.
- It is **very unlikely** that as an overt CCTV system, we would be asked to assist with an intrusive surveillance.
- III** An agreed protocol incorporating the use of RIPA where required is provided (agreed by the Police and Newark and Sherwood District Council) to cover the use of the camera system by the Police for targeted or specific investigations and operations (the Protocol is maintained within the CCTV Control Room).
- IV** Directed surveillances must be authorised and managed in accordance with the agreed protocol. The Corporate Manager- Risk and Resilience Manager or his/her nominated Officer, will be informed of every authorised surveillance that is to be carried out which involves the use of cameras managed by Newark & Sherwood District Council. He/she will ensure that authorisation and the following of agreed protocol has been made before permission is given for such surveillance to commence.
- V** An intrusive surveillance must be authorised in writing, by a Chief Constable.
- VI** It is the responsibility of the authorising Officer to review the ongoing surveillance activities and cancel when appropriate. Such cancellation must be informed to the CCTV operator. The Police will maintain overall responsibility for the surveillance.
- VII** A Police Officer will normally be present in the Control Room throughout the duration of the directed/intrusive surveillance and may operate the camera or direct the CCTV operator with the agreement of the Corporate Manager- Risk and Resilience or his deputy.
- VIII** Upon commencement of any Police surveillance, details, including the attending Officer, authorising Officer, location, reasons for the surveillance, dates and times and the unique surveillance number, will be entered onto the CCTV operators' log sheet, prior to the commencement of the surveillance.
- IX** The use of town centre CCTV systems is not normally regulated by the Act (RIPA). This is because members of the public are aware that these systems are in existence and are there for their own protection and to assist in preventing and detecting crimes. However where specific targeted operations are undertaken RIPA will apply.
- X** Directed and Intrusive surveillances will also be authorised by designated Officers within Newark & Sherwood District Council for Council managed operations. Directed surveillance's can be authorised by a Head of Department and above. Intrusive surveillance will only be authorised by a Chief Executive Officer.

- XI** Elected Members are not authorised to instruct any surveillance procedures and they must refer their requests through to the designated Officers within the Council.
- XII** No surveillances, whether directed or intrusive, Police or Newark & Sherwood District Council led, will be carried out without first informing the Corporate Manager- Risk and Resilience in order to allow CCTV to assist them.
- XIII** When a RIPA is authorised all the CCTV data gathered from the authorised investigation must be kept by the requester for a minimum of 5 years including non evidential footage. The requesting authority will therefore need to supply a corresponding number of digital storage hard drives at 1 TB per day of authorised use (whole system) or state the actual cameras to be used on the RIPA authority so that a lesser amount of storage is required.
- XIV** The Nottinghamshire Police contact point for information and advice on RIPA is the Covert Authority Bureau via the Police main switchboard. The CAB will authorize all Police RIPA activity via CCTV and confirm the validity of each by e-mail.

## Section 11

### Mobile CCTV

#### I Guiding Principles

For the purposes of this Code "Mobile CCTV" means any CCTV equipment, which is not permanently fixed in position, including CCTV Mobile vans and moveable street mounted cameras and fly-tipping systems.

#### II Introduction

The purpose of this section is to ensure that emerging systems such as mobile CCTV vehicles (normally a marked CCTV van) or deployable static cameras (temporarily fixed in position) operate in a way that is compliant with all legal requirements. It is essential that evidence obtained using such equipment is acceptable and admissible by the courts. These systems being relatively new may initially provide the opportunity for legal challenge when used to gather evidence towards a possible conviction. The intention of this section is to ensure that wherever possible opportunities to challenge the use of mobile equipment in the courts are minimised.

#### III Deployment

Regardless of whether the cameras are positioned for a very short time (in a stationary vehicle), or whether they are fixed for longer periods, such as those temporarily attached to street furniture. Consideration must be given to the restrictions placed by the Data Protection Act and possible infringements of Human Rights, in particular Article 8 - the right to private life.

#### IV Initial Siting Assessment Procedures:

- a) The Data Protection Act requires that an Initial Assessment is carried out by the organisation legally responsible for the System before CCTV systems are deployed. In this case the person or organisation legally responsible for the System would be (jointly) the Local Authority and Nottinghamshire Police (assuming the equipment used is either jointly funded, jointly operated or jointly agreed through a Community Safety Partnership). There will also be joint Data Controllers, with responsibilities as managers devolved to the appropriate Liaison Officer / CCTV manager from each organisation. The decision to deploy the cameras must be based on Crime Patterns and or Criminal Intelligence, both of which should have supporting data.
- b) The appropriateness for the siting and deployment of mobile / transportable CCTV equipment must be supported by written crime patterns analysis and / or reference to criminal intelligence logs. Reference to this must be made in writing on the CCTV Deployment Log, together with the purpose of the installation / deployment which will be one of the following:
  - i) Prevention, investigation and /or detection of crime
  - ii) Apprehension and /or prosecution of offenders
  - iii) Public and employee safety
  - iv) Staff discipline
  - v) Traffic flow monitoring (only needed if processing personal data).
- c) Covert operations will, however, be undertaken for fly-tipping in accordance with Human Rights and Data Protection Acts.

**V Siting Cameras**

The siting of cameras, especially where cameras could potentially intrude into domestic areas such as gardens, will normally require consultation with those affected. If this is not possible, for instance, when doing so would prevent the purpose of the deployment becoming ineffectual, then this should be recorded. Where cameras invade private space, electronic restrictions should be applied if possible, and in any case operators must be made aware of their responsibilities under the Data Protection Act and Human Rights Act (see also training requirements).

**VI Signage**

The requirement for signage of CCTV schemes is covered under the Data Protection Act Codes of Practice. Clearly providing appropriate signs with such portable systems will have its difficulties. Vehicles must be sign written with the appropriate information as defined in the Data Protection Act Codes of Practice. In the case of transportable systems, temporary signs (worded appropriately) should be positioned / erected on the approach to the areas where the cameras have been temporarily installed. These must be removed at the same time as the cameras are removed. Signs erected for periods of any length of time may require planning permission. Signage would not apply for covert operations.

**VII Staffing**

The staffing of mobile units varies in differing parts of the country. In the main these systems are operated either by Local Authority staff (contract or otherwise) or Police staff.

**VIII Training**

In all cases, selection of the staff used to operate such equipment should follow the same requirements for the selection, recruitment and training of CCTV operators. They must also receive specific training in respect of Human Rights, Data Protection, Regulation of Investigatory Powers Act, Freedom of Information Act and Police & Criminal Evidence Act in the context of the use of CCTV equipment.

## Appendix A

### Key Personnel and Responsibilities

#### I NEWARK AND SHERWOOD DISTRICT COUNCIL

Tel: 01636 650000

##### a) Responsibilities:

NEWARK AND SHERWOOD DISTRICT COUNCIL is the 'owner' of the system. The nominee will be the single point of reference on behalf of the owner. Their role will include a responsibility to:

- i) Ensure the provision and maintenance of all equipment forming part of the Newark CCTV System in accordance with contractual arrangements which the owner may from time to time enter into.
- ii) Maintain close liaison with the System manager.
- iii) Ensure the interests of Newark and Sherwood District Council and other organisations are upheld in accordance with the terms of this Code of Practice.
- iv) In partnership with the System manager, agree to any proposed alterations and additions to the system, this Code of Practice and/or the Procedural Manual.

#### II Management

##### CORPORATE MANAGER RISK & RESILIENCE, NEWARK AND SHERWOOD DISTRICT COUNCIL

Tel: 01636 650000

##### a) Responsibilities:

NEWARK AND SHERWOOD DISTRICT COUNCIL is the 'manager' of the system and 'data controller'. The nominee, the Corporate Manager of Risk & Resilience, will be the single point of reference on behalf of the manager. His/her role will include a responsibility to:

- i) Maintain day to day management of the system and staff.
- ii) Accept overall responsibility for the system and for ensuring that this Code of Practice is complied with.
- iii) Maintain direct liaison with the owner of the system.

## Appendix B

### Extracts from the Data Protection Act, 1998

#### Section 7

- (1) Subject to the following provisions of this section and to sections 8 and 9, an individual is entitled:
  - (a) To be informed by any data controller whether personal data of which that individual is the data subject is being processed by or on behalf of that data controller.
  - (b) If that is the case, to be given by the data controller a description of:
    - (i) The personal data of which that individual is the data subject.
    - (ii) The purpose for which they are being or are to be processed.
    - (iii) The recipients or classes of recipients to whom they are or may be disclosed.
  - (c) To have communicated to him/her in an intelligible form:
    - (i) The information constituting any personal data of which that individual is the data subject, and
    - (ii) Any information available to the data controller as the source of that data, and
  - (d) Where the processing by automatic means of personal data of which that individual is the data subject for the purposes of evaluating matters relating to him/her such as, for example, his/her performance at work, his/her creditworthiness, his/her reliability or his/her conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him/her, to be informed by the data controller of the logic involved in that decision-making.
- (2) A data controller is not obliged to supply any information under subsection (1) unless he/she has received:
  - (a) A request in writing, and
  - (b) Except in prescribed cases, such fee (not exceeding the prescribed maximum) as he/she may require.
- (3) A data controller is not obliged to comply with a request under this section unless he/she is supplied with such information as he/she may reasonably require in order to satisfy him/herself as to the identity of the person making the request and to locate the information which that person seeks.
- (4) Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he/she is not obliged to comply with the request unless: (a) the other individual has consented to the disclosure of the information to the person making the request, or (b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual.
- (5) In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request; and that subsection is not to be construed as excusing the data controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by omission of names or other identifying particulars or otherwise.

- (6) In determining for the purposes of subsection (4)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular, to:
- a) Any duty of confidentiality owed to the other individual.
  - b) Any steps taken by the data controller with a view to seeking the consent of the other individual.
  - c) Whether the other individual is capable of giving consent, and
  - d) Any express refusal of consent by the other individual.
- (7) An individual making a request under this section may, in such cases as may be prescribed, specify that his/her request is limited to personal data of any prescribed description.
- (8) Subject to subsection (4), a data controller shall comply with a request under this section promptly and in any event before the end of the prescribed period beginning with the relevant day.
- (9) If a court is satisfied on the application of any person who has made a request under the subsequent provisions of this section that the data controller in question has failed to comply with the request in contravention of those provisions, the court may order him/her to comply with the request.
- (10) In this section:
- ‘prescribed’ means prescribed by the Secretary of State by regulations.
  - ‘the prescribed maximum’ means such amount as may be prescribed.
  - ‘the prescribed period’ means forty days or such other period as may be prescribed.
  - ‘the relevant day’, in relation to a request under this section, means the day on which the data controller receives the request or, if later, the first day on which the data controller has both the required fee and the information referred to in subsection (3).
- (11) Different amounts or periods may be prescribed under this section in relation to different cases.

## 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;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 is processed and the frequency with which the data is 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 a 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.

Note: These extracts are for guidance only. To ensure compliance with the legislation, the relevant Data Protection legislation should be referred to in its entirety.

## Appendix C

### National Standard for the Release of Data to Third Parties

#### I General Policy

- a) It is strongly recommended that local procedures should be put in place to ensure a standard approach to all requests for the release of data. It is recommended that every request is channelled through the data controller<sup>(1)</sup>.

Notes:

- (1) The **data controller** is the person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal data is, or is to be, processed. (In most cases the data controller is likely to be the scheme owner or manager).

#### II Primary Request to View Data

- a) Primary requests to view data generated by a CCTV System are likely to be made by third parties for any one or more of the following purposes:
- i) Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996, etc.).
  - ii) Providing evidence in civil proceedings or tribunals.
  - iii) The prevention of crime.
  - iv) The investigation and detection of crime (may include identification of offenders).
  - v) Identification of witnesses.
- b) Third parties, which should be required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:
- i) Police <sup>(1)</sup>.
  - ii) Statutory authorities with powers to prosecute, (e.g. Customs and Excise; Trading Standards, etc).
  - iii) Solicitors <sup>(2)</sup>.
  - iv) Plaintiffs in civil proceedings<sup>(3)</sup>.
  - v) Accused persons or defendants in criminal proceedings <sup>(3)</sup>.
  - vi) Other agencies, (which should be specified in the Code of Practice) according to purpose and legal status<sup>(4)</sup>.
- c) Upon receipt from a third party of a bona fide request for the release of data, the scheme owner (or representative) should:
- i) Not unduly obstruct a third party investigation to verify the existence of relevant data.
  - ii) Ensure the retention of data which may be relevant to a request, but which may be pending application for, or the issue of, a court order or subpoena, (it may be appropriate to impose a time limit on such retention which should be notified at the time of the request).

- d) In circumstances outlined at note (3) below, (requests by plaintiffs, accused persons or defendants) the owner (or nominated representative) should:
- i) Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.
  - ii) Treat all such enquiries with strict confidentiality.

**Notes:**

- (1) The release of data to the police may not be restricted to the civil police but could include (for example) British Transport Police, Ministry of Defence Police, Military Police, etc (it may be appropriate to put in place special arrangements in response to local requirements).
- (2) Aside from criminal investigations, data may be of evidential value in respect of civil proceedings or tribunals. In such cases a solicitor, or authorised representative of the tribunal, should be required to give relevant information in writing prior to a search being granted. In the event of a search resulting in a requirement being made for the release of data, such release will only be facilitated on the instructions of a court order or subpoena (it may be considered appropriate to make a charge for this service). In all circumstances data will only be released for lawful and proper purposes.
- (3) There may be occasions when an enquiry by a plaintiff, an accused person, a defendant or a defence solicitor falls outside the terms of disclosure or subject access legislation. An example could be the investigation of an alibi. Such an enquiry may not form part of a prosecution investigation. Defence enquiries could also arise in a case where there appeared to be no recorded evidence in a prosecution investigation.
- (4) The Scheme owner should decide which (if any) 'other agencies' might be permitted access to data. Having identified those 'other agencies', such access to data will only be permitted in compliance with this Standard.

### **III Secondary Request to View Data**

- a) A 'secondary' request for access to data may be defined as any request being made which does not fall into the category of a primary request. Before complying with a secondary request, the Scheme owner should ensure that:
  - i) The request does not contravene, and that compliance with the request would not breach, current relevant legislation (eg. Data Protection, Human Rights Act, section 163 Criminal Justice and Public Order Act 1994, etc).
  - ii) Any legislative requirements have been complied with (eg. the requirements of the Data Protection Act).
  - iii) Due regard has been taken of any known case law (current or past) which may be relevant (eg. R v Brentwood BC ex p. Peck see page 28) and
  - iv) The request would pass a test of 'disclosure in the public interest'<sup>(1)</sup>.
- b) If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards should be put in place before surrendering the material:
  - i) In respect of material to be released under the auspices of 'crime prevention', written agreement to the release of the material should be obtained from a police officer, not below the rank of Inspector. The officer should have personal knowledge of the circumstances of the crime/s to be prevented and an understanding of the CCTV System Code of Practice<sup>(2)</sup>.
  - ii) If the material is to be released under the auspices of 'public well being, health or safety', written agreement to the release of material should be obtained from a senior officer within the Local Authority. The officer should have personal knowledge of the

potential benefit to be derived from releasing the material and an understanding of the CCTV System Code of Practice.

- c) Recorded material may be used for bona fide training purposes such as police or staff training. Under no circumstances will recorded material be released for commercial sale of material for training or entertainment purposes.

Notes:

- (1) 'Disclosure in the public interest' could include the disclosure of personal data that:
  - i) Provides specific information which would be of value or of interest to the public well being.
  - ii) Identifies a public health or safety issue.
  - iii) Leads to the prevention of crime.
- (2) The disclosure of personal data which is the subject of a 'live' criminal investigation would always come under the terms of a primary request (see III above).

#### **IV Individual Subject Access under Data Protection Legislation**

- a) Under the terms of Data Protection legislation, individual access to personal data, of which that individual is the data subject, must be permitted providing:
  - i) The request is made in writing.
  - ii) A specified fee is paid for each individual search.
  - iii) The data controller is supplied with sufficient information to satisfy him or her self as to the identity of the person making the request.
  - iv) The person making the request provides sufficient and accurate information about the time, date and place to enable the data controller to locate the information which that person seeks (it is recognised that a person making a request is unlikely to know the precise time. Under those circumstances it is suggested that within one hour of accuracy would be a reasonable requirement).
  - v) The person making the request is only shown information relevant to that particular search and which contains personal data of her or him self only, unless all other individuals who may be identified from the same information have consented to the disclosure.
- b) In the event of the Scheme owner complying with a request to supply a copy of the data to the subject, only data pertaining to the individual should be copied (all other personal data which may facilitate the identification of any other person should be concealed or erased). Under these circumstances an additional fee may be payable.
- c) The owner is entitled to refuse an individual request to view data under these provisions if insufficient or inaccurate information is provided (however every effort should be made to comply with subject access procedures and each request should be treated on its own merit).
- d) In addition to the principles contained within the Data Protection legislation, the data controller should be satisfied that the data is:
  - i) Not currently and as far as can be reasonably ascertained, not likely to become, part of a 'live' criminal investigation.
  - ii) Not currently and as far as can be reasonably ascertained, not likely to become, relevant to civil proceedings.

- iii) Not the subject of a complaint or dispute which has not been auctioned.
- iv) The original data and that the audit trail has been maintained.
- v) Not removed or copied without proper authority.
- vi) For individual disclosure only (i.e. to be disclosed to a named subject).

## V Process of Disclosure:

- a) Verify the accuracy of the request.
- b) Replay the data to the requestee only (or responsible person acting on behalf of the person making the request).
- c) The viewing should take place in a separate room and not in the control or monitoring area. Only data which is specific to the search request should be shown.
- d) It must not be possible to identify any other individual from the information being shown (any such information must be blanked-out, either by means of electronic screening or manual editing on the monitor screen<sup>(1)</sup>).
- e) If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material should be sent to an editing house for processing prior to being sent to the requestee.

Note:

- (1) The Scheme owner is likely to breach Data Protection legislation if a person making a subject access request is able to identify any other individual from the information being disclosed. However a television image is two dimensional and the majority of CCTV schemes do not have immediate access to the necessary technology to blank out or remove 'other data'. It is recommended that the advice of the Data Protection Registrar's office is sought in respect of any method which it is proposed should be adopted.

## VI Media Disclosure

- a) In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' should be followed. If material is to be released the following procedures should be adopted:
  - i) The release of the material must be accompanied by a signed release document that clearly states what the data will be used for and sets out the limits on its use.
  - ii) The release form should state that the receiver must process the data in a manner prescribed by the data controller, eg. specify identities/data that must not be revealed.
  - iii) It may also require that proof of editing must be passed back to the data controller, either for approval or final consent, prior to its intended use by the media (protecting the position of the data controller who would be responsible for any infringement of Data Protection legislation and the System's Code of Practice).
  - iv) The release form should be considered a contract and signed by both parties<sup>(1)</sup>.

Notes:

- (1) In the well publicised case of R v Brentwood Borough Council, ex parte Geoffrey Dennis Peck, (QBD November 1997), the judge concluded that by releasing the video footage, the Council had not acted unlawfully. A verbal assurance that the broadcasters would mask the identity of the individual had been obtained. Despite further attempts by the Council to ensure the identity would not be revealed, the television company did in fact broadcast footage during which the identity of Peck was not concealed. The judge concluded that tighter guidelines should be considered to avoid accidental broadcast in the future.

## **VII Principles**

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

- a) Recorded material should be processed lawfully and fairly and used only for the purposes defined in the Code of Practice for the CCTV Scheme.
- b) Access to recorded material should only take place in accordance with this Standard and the Code of Practice.
- c) The release or disclosure of data for commercial or entertainment purposes should be specifically prohibited.

## Appendix D

### Example of Restricted Access Notice

# **WARNING ACCESS TO THIS AREA IS RESTRICTED**

**Everyone, regardless of status, entering this area is required to complete an entry in the visitors log on the computer system.**

**Visitors are advised to note the following confidentiality clause and entry is conditional on acceptance of that clause.**

#### **Confidentiality clause:**

***'In being permitted entry to this area you are acknowledging that the precise location of the CCTV monitoring room is and should remain, confidential. You agree not to divulge any information obtained, overheard or overseen during your visit.***

***An entry accompanied by your signature in the visitors log is your acceptance of these terms'.***

## Appendix E

### Example of Declaration of Confidentiality

#### The NEWARK and SHERWOOD CCTV System

I, (.....) am retained by (.....) to perform the duty of CCTV operator / manager (or other authorised role as appropriate). I have received a copy of the Code of Practice in respect of the operation and management of that CCTV System.

I hereby declare that:

I am fully conversant with the content of that Code of Practice and understand that all duties which I undertake in connection with the (.....) must not contravene any part of the current Code of Practice, or any future amendments of which I am made aware. If now, or in the future, I am or become unclear of any aspect of the operation of the System or the content of The Code of Practice, I undertake to seek clarification of any such uncertainties.

I understand that it is a condition of my employment that I do not disclose or divulge to any individual, firm, company, authority, agency or other organisation, any information which I may have acquired in the course of, or for the purposes of, my position in connection with the CCTV System, verbally, in writing or by any other media, now or in the future (including such time as I may no longer be retained in connection with the CCTV System).

In appending my signature to this declaration, I agree to abide by the Code of Practice at all times. I also understand and agree to maintain confidentiality in respect of all information gained during the course of my duties, whether received verbally, in writing or any other media format - now or in the future.

Signed: ..... Print Name: .....

Witness: ..... Position: .....

Dated the ..... day of .....

## Appendix F

### Inspector's Declaration of Confidentiality in respect of the Newark and Sherwood CCTV System

I, (.....) am a voluntary inspector of the ( ..... ) CCTV System with a responsibility to monitor the operation of the System and adherence to the Code of Practice. I have received a copy of the Code of Practice in respect of the operation and management of that CCTV System.

I hereby declare that:

I am fully conversant with my voluntary duties and the content of that Code of Practice. I undertake to inform the System manager (*and/or the system owner*) of any apparent contraventions of the Code of Practice that I may note during the course of my visits to the monitoring facility.

If now, or in the future I am, or I become unclear of any aspect of the operation of the System or the content of The Code of Practice, I undertake to seek clarification of any such uncertainties.

I understand that it is a condition of my voluntary duties that I do not disclose or divulge to any firm, company, authority, agency, other organisation or any individual, any information which I may have acquired in the course of, or for the purposes of, my position in connection with the CCTV System, verbally, in writing or by any other media, now or in the future (including such time as I may no longer be performing the role of inspector).

In appending my signature to this declaration, I agree to abide by the Code of Practice at all times. I also understand and agree to maintain confidentiality in respect of all information gained during the course of my voluntary duties, whether received verbally, in writing or any other media format - now or in the future.

Signed: ..... Print Name: .....

Witness: ..... Position: .....

Dated the ..... day of .....

**Subject Access Request Form****Appendix G****NEWARK & SHERWOOD DISTRICT COUNCIL CCTV SURVEILLANCE SYSTEM  
Data protection Act, 1998****HOW TO APPLY FOR ACCESS TO INFORMATION HELD ON  
THE CCTV SYSTEM**

These notes explain how you can find out what information, if any, is held about you on the CCTV system.

**Your Rights**

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or if you agree otherwise. Newark & Sherwood District Council will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, the Council is not obliged to comply with an access request unless:

- The other individual has consented to the disclosure of information, or
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual(s).

**Newark & Sherwood CCTV System Rights**

Newark & Sherwood District Council may deny access to information where the Act allows. The main exemptions in relation to information held on the CCTV System are where the information may be held for:

- Prevention and detection of crime
- Apprehension and prosecution of offenders

And giving you the information may be likely to prejudice any of these purposes.

**Fee**

A fee of £10 is payable for each access request, which must be in pounds sterling. Cheques, Postal Orders, etc. should be made payable to 'Newark & Sherwood District Council'.

**THE APPLICATION FORM:**

**(N.B. ALL sections of the form must be completed. Failure to do so may delay your application.)**

**Section 1** Asks you to give information about yourself that will help the Council to confirm your identity. The Council has a duty to ensure that information it holds is secure and it must be satisfied that you are who you say you are.

**Section 2** Asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, date of birth and current address) together with a recent full face photograph of you.

**Section 3** Asks you to confirm whether you will accept just viewing the information, or if you want a copy of the information.

**Section 4** **You must sign the declaration**

When you have completed and checked this form, take or send it together with the required TWO identification documents, photograph and fee to: THE CCTV MANAGER, Newark & Sherwood District council, Kelham Hall, Kelham, Newark, Notts NG23 5QX. or take it to any main Council Office in this District.

If you have any queries regarding this form, or your application, please ring  
The CCTV Manager on Tel No. 01636 655933.

**NEWARK & SHERWOOD DISTRICT COUNCIL CCTV SURVEILLANCE SYSTEM**  
**Data Protection Act 1998**

**SECTION 1                      About Yourself**

*The information requested below is to help the Council (a) satisfy itself as to your identity and (b) find any data held about you.*

**PLEASE USE BLOCK LETTERS**

<b>Title (tick box as appropriate)</b>	<i>Mr</i>	<input type="checkbox"/>	<i>Mrs</i>	<input type="checkbox"/>	<i>Miss</i>	<input type="checkbox"/>	<i>Ms</i>	<input type="checkbox"/>
<i>Other title (e.g. Dr., Rev., etc.)</i>								
<i>Surname/family name</i>								
<i>First names</i>								
<i>Maiden name/former names</i>								
<b>Sex (tick box)</b>	<i>Male</i>			<input type="checkbox"/>	<i>Female</i>			<input type="checkbox"/>
<i>Height</i>								
<i>Date of Birth</i>								
<i>Place of Birth</i>	<i>Town</i>							
	<i>County</i>							

<b>Your Current Home Address (to which we will reply)</b>								
	<i>PostCode</i>							
	<i>Tel. No.</i>							
<i>A telephone number will be helpful in case you need to be contacted.</i>								

*If you have lived at the above address for less than 10 years, please give your previous addresses for the period:*

<i>Previous address(es)</i>								
<i>Dates of occupancy</i>	<i>From:</i>				<i>To:</i>			

## NEWARK & SHERWOOD DISTRICT COUNCIL CCTV SURVEILLANCE SYSTEM Data Protection Act, 1998

### SECTION 2 Proof of Identity

*To help establish your identity your application must be accompanied by TWO official documents that between them clearly show your name, date of birth and current address.*

*For example: a birth/adoption certificate, driving licence, medical card, passport or other official document that shows your name and address.*

*Also a recent, full face photograph of yourself.*

*Failure to provide this proof of identity may delay your application.*

### SECTION 3 Supply of Information

*You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to:*

(a) *View the information and receive a permanent copy*

YES / NO

(b) *Only view the information*

YES / NO

### SECTION 4 Declaration

**DECLARATION** *(to be signed by the applicant)*

*The information that I have supplied in this application is correct and I am the person to whom it relates.*

*Signed by*

*Date*

*Warning – a person who impersonates or attempts to impersonate another may be guilty of an offence.*

*After completing Section 4 please review the 'CHECK' box on the last page before returning the form.*

**NEWARK & SHERWOOD DISTRICT COUNCIL CCTV SURVEILLANCE SYSTEM  
Data Protection Act, 1998**

**SECTION 5 To Help us Find the Information**

*If the information you have requested refers to a specific offence or incident, please complete this Section.*

*Please complete a separate box in respect of different categories/incidents/involvement. Continue on a separate sheet, in the same way, if necessary.*

*If the information you require relates to a vehicle, property, or other type of information, please complete the relevant section overleaf.*

Were you: (tick box below)

*A person reporting an offence or incident*

*A witness to an offence or incident*

*A victim of an offence*

*A person accused or convicted of an offence*

*Other – please explain*


**Date(s) and time(s) of incident**

**Place incident happened**

**Brief details of incident**

**NEWARK & SHERWOOD DISTRICT COUNCIL CCTV SURVEILLANCE SYSTEM  
Data Protection Act, 1998**

**CHECK BOX**

*Before returning this form*

- *Have you completed ALL Sections in this form?*

*Please check:*

- *Have you enclosed TWO identification documents?*
- *Have you signed and dated the form?*
- *Have you enclosed the £10.00 (ten pound) fee?*

**Further Information:**

*These notes are only a guide. The law is set out in the Data Protection Act, 1998, obtainable From The Stationery Office. Further information and advice may be obtained from:*

*The Information Commissioner,  
Wycliffe House,  
Water Lane,  
Wilmslow,  
Cheshire,  
SK9 5AF.  
Tel. (01625) 545745*

*Please note that this application for access to information must be made direct to Newark & Sherwood district Council (address on Page 1) and **NOT** to the Data Protection Commissioner.*

**OFFICIAL USE ONLY**

**Please complete ALL of this Section (refer to 'CHECK' box above).**

*Application checked and legible?*

*Date Application Received*

*Identification documents checked?*

*Fee Paid*

*Details of 2 Documents (see page 3)*

*Method of Payment*

*Documents Returned?*

*Receipt No.*



*Documents Returned?*

**Member of Staff completing this Section**

**Name**

**Location**

**Signature**

**Date**

## Appendix H

### MOBILE CCTV ADVISORY/LOAN FORM

#### Introduction

1. The Mobile CCTV system, jointly operated by Newark & Sherwood District Council and Nottinghamshire Police, is subject to the regulations detailed by the Data Protection Act 1998 Codes of Practice for users of CCTV and the Newark & Sherwood CCTV scheme Codes of practice. Mobile CCTV equipment users must familiarise themselves with these documents and ensure that the operation of this equipment remains within these guidelines.

2. In order to comply with the Data Protection Act, CCTV regulations, a site survey of the area to be monitored must be carried out. Any subsequent decision to use CCTV must be based on crime patterns or criminal intelligence, both of which should have supporting data. Operators should also have training in regulations pertaining to the use of CCTV including, the Human Rights Act, Data Protection Act, Regulation of Investigatory Powers Act, Freedom of Information Act and Police and Criminal Evidence Act.

#### Equipment Use

3. The mobile CCTV equipment/Mobile Van are expensive to purchase and maintain, for that reason care must be taken to ensure that the equipment is looked after. Faults or damage must be recorded so that they can be corrected or repaired as quickly as possible to prevent down time and loss of use.

#### Operators Log

4. In order to maintain continuity of evidence the equipment operators should maintain a log of CCTV operations (a log is provided for the CCTV Van, the 2.4 Ghz case and 1.3 Ghz Case). These logs should be used to detail the nature and location of the CCTV operation, the names of CCTV operators if any and details of any incidents monitored. Failure to keep an accurate log of events could prejudice any resultant court case if CCTV evidence from the operation is used.

#### CCTV Signs

5. As detailed in the Data Protection Act, whenever overt CCTV monitoring is being carried out, appropriate CCTV warning signs must be displayed. The signs must show that CCTV is in operation in the area, give the name of the organisation operating the system and give their contact details/phone number. Signs are not required when authority for Directed surveillance or Intrusive surveillance has been granted by the appropriately ranked police inspector in advance.

#### Loan Period

6. The Mobile CCTV equipment, 2.4 Ghz/1.3Ghz and Mobile Van are booked out in advance by various agencies. Therefore the equipment must be collected on the first day of the loan period and returned to Newark & Sherwood District Council by the agreed last day of the loan period or a further period of loan agreed prior to the return date.

#### Declaration

8. I have read the Newark & Sherwood District Council Mobile CCTV advisory/loan form and am aware of the regulations and Codes of Practice concerning the use of CCTV equipment or I am collecting the equipment on behalf of a third party and I will give them a copy of the advisory/loan form.

Name:.....

Position:.....

Signature:.....

# Appendix I

## CCTV Equipment Booking Out Form

Person responsible for equipment:.....

Contact number for person:.....

Date equipment loaned:.....

### 1.3 GHz Camera system

- Control Case
- 1.3 GHz camera (including mains lead)
- Tripod(s)
- YAGI directional antenna
- Battery charger
- Pole mount batteries
- Battery packs with handles for control case
- Battery to camera power leads
- Vehicle power point to control case lead
- Battery to control case power lead
- Mains to case transformer
- YAGI Leads

### 2.4 GHz Camera system

- Control Case
- 2.4 GHz camera (including mains lead)
- Tripod(s)
- Directional/ gain antenna
- Battery charger
- Pole mount batteries
- Battery packs with handles for control case
- Battery to camera power leads
- Vehicle power point to control case lead
- Battery to control case power lead
- Mains to case transformer
- Aerial Leads

Portable VCR  Portable Monitor  Mains power transformer  Leads

Tape numbers:

Intended use of equipment: Overt Crime prevention/Directed surveillance/Intrusive surveillances or other

Details:

All equipment has been returned. There is/is no damage or loss to report.

Signed: ..... Date

Checked By:..... Date

Damage noted:.....

Details: