Code of Practice

In respect of the operation of

Closed Circuit Television

Newport City Council

Law & Regulation

Public Protection Service

Community Safety

Civic Centre

NEWPORT

NP20 4UR

February 2016

CHANGE CONTROL RECORD

Date	Reference	Comment	By

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

Registration Number Z7916047

Contents

Section 1- Introduction and Objectives

Section 2- Statement of Purpose and Principles

Section 3- Privacy and Data Protection

Section 4- Accountability and Public Information

Section 5- Assessment of the System and Code of Practice

Section 6- Human Resources

6.1 Staffing of the Monitoring Room
6.2 Discipline
6.3 Rules of Conduct
6.4 Staff Recruitment
6.5 Security Screening
6.6 Human Rights statement
6.7 Training
6.8 Declaration of conformity
6.9 Health

Section 7- Control and Operation of Cameras

7.1 Guiding principles
7.2 Primary Control
7.3 Secondary Control
7.4 Operation of the system by the Police
7.5 Maintenance of the system

Section 8- Access to and security of the room

8.1 Authorised access
8.2 Public access
8.3 Authorised visits
8.4 Declaration of Confidentiality
8.5 Security
8.6 Emergency evacuation procedure

Section 9- Management of Recorded material

9.1 Guiding principles
9.2 Evidential Recordings

Section 10- Video Prints

Section 11- Communications

Appendices

A1- Key personnel
A2- Stakeholders
B- Standard for the release of data to third parties
C- Restricted access notice
D- Declaration of Confidentiality
E- Subject access request form
F- Regulation of Investigatory Powers Act 2000- Guiding principles
G1- Civil liberties
G2- Human Rights Act 1998

1.1 Introduction

A Closed Circuit Television (CCTV) system has been introduced to both Newport City Council and Blaenau Gwent Council.

This system, known as the Newport City Council CCTV, Newport IP CCTV System and Blaenau Gwent Council CCTV, comprises a number of cameras installed at fixed strategic locations. The cameras are predominantly pan and tilt with zoom facilities. The images from which are presented to an authorised CCTV Central Control Room. A single monitor is presented at the Gwent Police Control Room where Police can view incidents under the control and supervision of staff from the Council Control Room. The Police may also monitor the CCTV images under the authority of the Regulation of Investigatory Powers Act 2000 referred to as a RIPA Authority.

The 'System Owner' for CCTV imagery within the city of Newport is Newport City Council (NCC) and for Blaenau Gwent it is Blaenau Gwent County Borough Council (BGCBC).

For the purposes of the Data Protection Act, 1998 the 'data controller' is Newport City Council. (Note1.) The 'system manager' is Newport City Council.

The Newport City Council CCTV system has been notified to the Information Commissioner (Registration Number **(Z7916047**).

Note 1. The **data controller** is the person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are to be processed. It must be a legal entity e.g. person, organisation or corporate body and in the case of partnerships all partners may be considered to bear the responsibility.

1.2 Statement in respect of The Human Rights Act 1998

1.2.1 It is recognised that public authorities and those organisations carrying out 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 the City of Newport and Blaenau Gwent is necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety. (See 1.2.4 and 1.3 below)

1.2.2 This assessment is bound by Section 163 of the Criminal Justice and Public Order Act 1994 which 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.

1.2.3 It is recognised that operation of the NCC and BGCBC CCTV Surveillance System may be considered to infringe on the privacy of individuals. NCC recognises that it is

their responsibility to ensure that the scheme should always comply with all relevant legislation, to ensure its legality and legitimacy.

1.2.4 The scheme will only be used as a proportional response to identified problems and be used only in so far as it is necessary in a democratic society, in the interests of national security, public safety, the economic wellbeing 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.

1.2.5 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 fair trial.

1.2.6 The Newport City Council and Blaenau Gwent CCTV System shall be operated within the parameters set out by the European Convention on Human Rights.

1.3 Objectives of the System

1.3.1 To support the Police in a bid to deter and detect crime, identify apprehend and prosecute offenders

1.3.2 To reduce the levels of street crime, vandalism, public disorder, theft of and from cars both on public streets and in public car parks

1.3.3 To reduce the levels of graffiti and other criminal damage, thus improving the environment and reducing costs

1.3.4 To assist other emergency services

1.3.5 To increase personal safety and reduce the fear of crime

1.3.6 To assist the Local Authority in its efficient management, enforcement and regulatory functions of the Newport City Council and Blaenau Gwent areas covered by the CCTV System

1.3.7 To improve commercial confidence in the City

1.3.8 To prevent mitigating interruptions of traffic flows (not to enforce breaches of traffic law)

1.3.9 Identifying and preventing racial harassment

1.3.10 The System will safeguard the privacy of individuals and not invade the privacy of any individual in residential, business or other private premises, building or and unless in-direct pursuance of objectives 1.3.2 to 1.3.7 inclusive

1.3.11 The System will only be used for the defined purposes; any additional requests for use of the system will be individually assessed in relation to RIPA or criminal prosecutions.

1.4 System Ancillary Uses

1.4.1 Hotspot or vulnerable areas monitored to allay public concern about safety and enable effective response to incidents

1.4.2 To promote the effective use of Store and Night Net radio communications systems to assist in the reduction of business crime

1.4.3 To provide production of evidential material for Crown Prosecution Services

1.4.4 Reporting anti-social behaviour to the Community Safety Wardens via Tetra Radio on all incidents reported by police and the public.

1.4.5 Provide monitoring and supervisory services for;

1.4.5.1 Silent Valley Lagoon monitoring in the prevention of sewage and toxic overflow

1.4.5.2 Provide CCTV monitoring of 'Remote' site locations such as council owned sites.

1.4.5.3 To provide traffic congestion reports over telephone and radio.

1.5 Procedural Manual

1.5.1 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 (see Section 2) of the CCTV system are realised, the procedural manual is based and expands upon the contents of this Code of Practice.

1.6 Normative References

1.6.1 All reference to the British Standards within the Code of Practice or Procedures manuals, relate to the latest publications;

British Standard (BS) 7958:2015- Closed circuit television (CCTV)-Management and operation-code of practice

British Standard (BS) 7858:2012 Security screening of individuals employed in a security environment- code of practice

1.6.2 ICO Code of Practice for surveillance cameras and personal information version 1.1 21/05/2015

1.6.3 H.O Surveillance Camera Code of Practice June 2013.

1.6.4 ICO Conducting Privacy Impact Assessments Code of Practice November 2014.

SECTION 2 STATEMENT OF PURPOSE AND PRINCIPLES

2.1 Purpose

The purpose of this document is to state the intention of the owners and the managers, on behalf of the partnership as a whole and as far as is reasonably practicable, to support the objectives of NCC CCTV System and BGCBC CCTV System, (hereafter referred to as 'The System') and to outline how is intended to do so

2.1.1 Enables local authorities to provide closed circuit television coverage of any land within their area for the purposes as set out above

2.1.2 The 'Purpose' of the System, 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

2.1.3 Policy and scheme review Annual Report (See BS 7958:2015) this document sets out the policy of NCC in respect of the management of the CCTV system in operation- and a review will take place annually (WEF 1.4.17) in respect of;

- Whether the objective statements remain valid
- Changes to the scope of the scheme
- Contracts with suppliers
- A review of the current data protection and legal requirements
- Maintenance schedule
- Report annually on performance

2.2 General Principles of Operation

1.6.5 2.2.1 The system will be operated in accordance with all the requirements and the principles of the Human Rights Act 1998 and the H.O Surveillance Camera Code of Practice June 2013.

2.2.2 Operation of the system will also recognise the need for formal authorisation of any covert 'Directed' surveillance of crime – trend ('hotspot') surveillance as required by the Regulation of Investigatory Powers Act 2000 and police force policy

2.2.3 The system will be operated fairly, within the law, and only for the purpose for which it was established and are identified within this Code, or which are subsequently agreed in accordance with this Code of Practise

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

2.2.5 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.

2.2.6 Discourage the unnecessary or inappropriate proliferation of CCTV in places without redress to an Operational Requirement

2.2.7 Evolve in line with technological and cultural change by means of regular review and development process

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

2.2.9 How to make complaint-third parties can make a complaint about the operation of this system by contacting Newport City Council telephone number 01633-656656 or via the NCC website (See the complaints procedure at Newport.gov.uk)

2.3 Copyright

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

2.4 CCTV Camera Area Coverage

2.4.1 The areas covered by CCTV to which this Code of Practice refers are the public areas within the responsibility of NCC and BGCBC

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 System and be governed by these Codes and Procedures

2.4.3 Camera capability are either fixed or of the pan/tilt/zoom variety

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

2.5 Monitoring and Recording Facilities

2.5.1 A staffed monitoring room is located at a secure location within the boundaries of Newport. The CCTV equipment has the capability of recording all cameras simultaneously throughout every 24 hour period

2.5.2 Newport secondary monitoring equipment can only be viewed via single monitor and is located at Gwent Police Headquarters incident control room, Croesyceiliog. 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 from selected cameras in real-time, produce hard copies of recorded images, replay or copy any pre-recorded data in accordance with the Code of Practice. All viewing and recording equipment shall only be operated by trained and authorised operators.

2.6 Human Resources

2.6.1 The monitoring room shall be staffed by SIA trained operators

2.6.2 All operators shall receive training relevant to their role.

2.7 Processing and Handling of Recorded Material

2.7.1 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.

2.8 Operators Instructions

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

2.9 Changes to the Code or the Procedural Manual (See also 2.1.3 above)

2.9.1 The systems Code of Practice and Procedural Manual will be reviewed once a year or whenever appropriate (i.e. new legislation, guidance or due to the development of 'Best Practice').

2.9.2 The systems owners NCC have authorised the Systems Manager to undertake responsibility for reviewing and amending changes to this document.

2.9.3 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 System Manager and the owners of the system.

Notes:

*i) 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*

ii) 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

iii) The use of 'dummy' cameras as part of a CCTV System is strongly discouraged. The greatest deterrent value of a CCTV System is its power to produce evidential material and, in doing so, to reassure those it is intended to protect

iv) None of the cameras forming part of Newport City Council CCTV System will be installed in a covert manner

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

Note: 'Processing means **obtaining, recording** or **holding** the information or data or **carrying out any operation** or **set of operations** on the information or data, including:

i) Organisation, adaptation or alteration of the information or data;
ii) Retrieval, consultation or use of the information or data;
iii) Disclosure of the information or data by transmission, dissemination or otherwise making available, or
iv) Alignment, combination, blocking, erasure or destruction or the information or data.

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.

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 **(Registration Number Z7916047**

3.2.2 The 'data controller' for The System is Newport City Council and day to day responsibility for the data will be devolved to CCTV System Manager Mr Christopher Norman, Telford Street, Newport, South Wales, NP19 0EF.

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
ix) A copy of the Data Protection Act, 1998 is held within the NCC Control Room and is available to all staff

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 System Manager or data controller. A Fee of £10 (Ten Pounds) is payable for each access request, which must be in GB Pounds sterling. Cheques etc. should be made payable to "Newport City Council",

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.

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 E.

3.3.5 Any person making a request should either be given a copy of the ICO code or details of the ICO Website

3.3.6 Requests for information also need to be aware of two further rights that individuals have under the DPA. Personnel need to recognise a request from an individual to prevent processing likely to cause substantial and unwarranted damage or distress (s10 DPA) and one to prevent automated decision-taking in relation to the individual (s12 DPA).

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
iii) Civil Proceedings 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'

Note: *Each and every application will be assessed on its own merits and general 'blanket exemptions' will not be applied. In every such case the System Manager or Data controller will liaise with the investigation Police Officer and CPS*

A Police Officer may request by arrangement with Control Room Staff to view any data, which he or she believes may be of evidential value in the prevention or detection of a crime. While control room staff may enable viewing of an incident, it is the duty of the investigating officer to ensure that material of potential evidential value is reviewed.

Once a disc has been reviewed by an officer, it should be seized in accordance with the Procedural Manual

Requests for copies of still Photographs from Police will only be considered when authorised by an Officer of at least the rank of Sergeant. All still photographs produced shall be identified with a unique sequential reference number and a record kept of reason for production, details of staff issuing, time and date.

Still Photographs shall only be produced for prevention and detection of crime and shall be treated as exhibits. Unless such photographs are requested for evidence, they should be destroyed within 31 days. A record shall be kept of such destruction. The National Standard for release of data to third parties shown at Appendix B must be complied with

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 monitoring 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

4.2 Complaints

4.2.1 All complaints shall be dealt with in accordance with Newport City Council complaints procedure, a copy of which may be obtained from Newport City Council website.

4.2.2 All CCTV staff are contractually subject to regulations governing confidentiality and discipline

4.3 System Owner

4.3.1 System Owners will ensure that System Managers and Data Controllers comply with Code of Practice and Procedural Manuals

4.4 System Manager

4.4.1 The System Manager will ensure that every complaint is acknowledged in writing within a reasonable time period 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 owner giving details of all complaints and the outcome of relevant enquiries.

4.5 Public Information: Freedom of Information Act 2000

4.5.1 The Freedom of Information Act 2000 gives a general right of access to all types of information held by public authorities, sets out exemptions from that right and places a number of obligations on public authorities. Any person who makes a request for information must be told whether the authority holds that information and subject to exemptions, supplied with the information requested

4.5.2 Clearly this would include recorded images of an individual, either during the storage period of a month (Maximum period allowed) or if the tape has been retained for longer or for a specific purpose.

4.5.3 Individuals already have the right of access to information about themselves under the Data Protection Act 1998. As far as public authorities are concerned, the Freedom of Information Act, 2000 will extend this to access all types of information held.

4.5.4 The Act will be enforced by the Surveillance Camera Code of Practice (June 2013) and the Information Commissioner ('the Commissioner'), a post that combines regulation of the Freedom of Information 2000 and the Data Protection Act 1998

4.5.5 **Code of Practice**

A copy of this Code of Practice shall be published on NCC web site

4.6 Signs

Signs (as shown below) will be placed in the locality of the cameras and at main entrance points to the relevant areas. The signs will indicate:

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

Defnyddir

CCTV

in Operation

for security and safety

ar gyfer gwarchod a diogelu

Operator/Gweithredwr	**Newport City Council**
	Cyngor Dinas
CasnewyddTelephone/Ffôn	**01633 656656**

Section 5 Assessment of the System and Code of Practice

5.1 Evaluation

5.1.1 Performance indicators will be produced to senior management within NCC and BGCB at agreed periods throughout the year

5.1.2 It is intended that evaluations will be carried out by line management (See 5.4)

5.2 Monitoring

5.2.1 The Senior CCTV operator (Supervisor) will accept day to day responsibility for the monitoring, operation and evaluation of the system and the implementation of this Code of Practice.

.

5.3 Audit

5.3.1 The NCC Chief internal auditor, or his/her nominated deputy, who is not the system manager 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 monitoring room records, DVD histories and the content of recorded material.

5.4 Inspection

5.4.1 There will be an annual inspection of the System, carried out by line management to ensure:-

(1) Equipment is being maintained in accordance with the agreed maintenance contract in place.

5.4.2 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. Their findings will be reported to the Auditor and their visit recorded in the CCTV monitoring room

5.4.3 Inspectors will be required to sign a declaration of confidentiality.

.

Section 6 Human Resources

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

6.1.1 The CCTV Monitoring Room will be staffed in accordance with both the Codes of Practice and 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 monitoring room procedures.

6.1.2 Every person involved in the management and operation of the system 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 Every person will be required to sign confirmation that they fully understand the obligations and adherence to these documents placed upon them. Failure by staff to comply with the Codes of Practice and Procedural Manuals will be considered Gross Misconduct under the Councils Disciplinary Code and may also result in criminal prosecution.

6.1.4 Equipment will only be operated by trained and authorised personnel. All staff will be required to have an SIA Licence.

6.1.5 All new personnel recruited shall be checked and vetted in accordance with local authority procedures. Completion of an induction programme and a suitable probationary period will be subject of validation of employment, health and other details.

6.1.6 All personnel involved with the system shall receive training from time to time in respect of all legislation appropriate to their role.

6.1.7 Arrangement may be made for a police liaison officer to be present in the monitoring room at certain time(s), or indeed at all times, subject to locally agreed protocols. Any such person must also be conversant with this Code of Practice and associated Procedural Manual.

6.1.8 CCTV Volunteer Scheme- CCTV Volunteers will be employed within the NCC Control Room as defined by the NCC Volunteers policy and will provide a supportive role to the full time paid staff within the room by undertaking duties that will allow the paid staff to monitor and provide CCTV images to the Police as a priority.

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 NCC discipline code.

6.2.2 NCC will reserve the right to run security checks, both at the interview stage and during employment against individuals who are employed to work within the CCTV environment.

6.3 Rules of Conduct

Our employers and the general public are entitled to expect the highest standards of conduct from all staff employed within the scheme. In performing their duties, they should act with probity, impartiality and objectively.

The following list of offences is not to be regarded as an exhaustive list. Acts of misconduct not falling within one or more of the rules may also rise to disciplinary action.

i) Neglecting to complete a required task at work promptly and diligently, without sufficient cause.

ii) Leaving the place of work without permission, or without sufficient cause.

iii) Making or signing of false statements of any description.

iv) Destroying, altering, erasing or removing documents, records or electronic data without permission or through negligence.

v) Permitting or participating in the bringing of unauthorised discs or digital formats pre-recorded or unrecorded into the CCTV Control Room.

vi) Permitting or participating in the bringing of unauthorised photographic equipment into the CCTV Control Room.

vii) Divulging matters confidential to the organisation or customer, either past or present, without permission.

viii) Soliciting or receipt of gratuities or other considerations from any person, or failure to account for keys, money, or property received in connection with the System.

ix) Incivility to persons encountered in the course of duties, or misuses of authority in connection with the System.

x) Conduct in a manner likely to bring discredit to Newport City Council CCTV Surveillance System, client or fellow employee.

xi) Using equipment or identification without permission.

xii) Reporting for duty under the influence of alcohol or restricted drugs, or use of these whilst on duty.

xiii) Failing to notify the System Manager immediately of any;

a) Convictions for a criminal and/or motoring offences
b) Indictment for any offences;
c) Police cautions; or
d) Legal summons;

xiv) Permitting unauthorised access to the CCTV control room or premises to any person.

xv) Carrying of equipment not issued as essential to an employee's duties, or use of customers equipment or facilities without permission.

xvi) Not maintaining agreed standards of appearance and deportment whilst at work.

xvii) Failure of the Systems operator to justify their reason for recording an individual or group of individuals, or property, when required to do so by the Systems manager or auditor.

xviii) Failure to notify the System manager of any periods of sickness or absenteeism.

xix) Failure of the System operator to ensure all duties are performed in accordance with the Scheme's Code of Practice and Operational Procedure Manuals;

xx) Failure by the System Manager to ensure the system operates accordance with the stated objectives and procedures contained within the Schemes Code of Practice and Operational Procedures Manuals.

6.4 Staff Recruitment and Selection

6.4.1 Recruitment and selection should be in accordance with or equivalent to BS 7858: 2006

6.5 Security Screening

6.5.1 BS 7858:2012 Employee Security- Screening of personnel employed in a security environment, will be complied with.

6.5.2 BS 7958:2015 Code of Practice and Management and Operation of CCTV will be complied with

6.5.2 Screening should apply to all personnel, irrespective of whether they are engaged full-time, on a part-time basis or volunteers.

6.6 Human Rights Statement

6.6.1 It is clear that the requirement for checking the background of staff employed in CCTV control rooms, does engage an individuals' Human Rights (Article 8 right to respect for private lift). We believe however that this is justified in order to ensure the honesty and integrity of the employee or prospective employee, bearing in mind they will be handling the data of the subjects of the CCTV operations, and therefore for the prevention of crime. The position of personnel involved in CCTV means they are privy to information that could put them in a position where they could abuse information for the purposes of crime. An applicant's character needs to be beyond reproach and should be viewed no differently than that of a police officer.

6.7 Training

6.7.1 In accordance with BS 7958:2015 5.3 all staff employed within the control room operating CCTV will be provided with the following training:

6.7.2 Induction training and pack that will include;

- Working conditions- see job profile/requirement
- Relevant health and safety within the CCTV control room
- Fire awareness training and evacuation
- Use of appropriate equipment
- Operation of appropriate equipment
- Management of recorded material
- Relevant legal issues and codes
- Privacy and disclosure
- Disciplinary code

.

6.7.2 All permanent and part-time staff will be required to complete a Security Industry Authority (SIA) training.

6.8 Declaration of Conformity

6.8.1 Every individual with any responsibility under the terms of this Code of Practice or who has any involvement with The System to which they refer, will be required to sign a declaration of confidentiality. See Appendix D, also Section 8 concerning access to the monitoring room by others).

6.9 Health

6.9.1 Prospective employees will be required to submit details of their medical history prior to employment and should be able to demonstrate

i) Good general health;
ii) Good eyesight (including colour vision), hearing and sense of smell.

6.9.2 They should be able to demonstrate good reading, writing and verbal communication abilities and be computer literate.

6.9.3 Where night-time working is involved, prospective employees should be asked to confirm that there is nothing in their circumstances that would be detrimental to their working night shifts. Night-time workers should be offered the opportunity of free annual medical assessments. In addition, Night-Timers workers will be required to complete a Health and Safety Night-Time Assessment Questionnaire. In order to ensure that the physical condition of control room operatives remains compatible with the duties to which they have been assigned.

6.9.4 All personnel will be required to undertake Display Screen Equipment screening and compliance

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 compliance 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 that 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.

7.1.6 The Regulation of Investigatory Powers Act 2000 "RIPA" was enacted simultaneously with the Human Rights Act, 1998 in order to control legitimate covert surveillance and undercover operations whilst undertaking criminal investigations.

7.1.7 This Act " RIPA" is only relevant if the investigation is covert. It will not, therefore, apply where the investigation is open and overt.

7.1.8 The following will be complied with; Protection of Freedoms Act- Conducting privacy impact assessments code of practice version 1.0 and Surveillance Camera Commissioner Code of Practice- steps to complying with the 12 principles. For more information- https://www.gov.uk/government/organisation/surveillence-camera-commissioner

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, those operators have primacy of control at all times.

7.2.2 When the CCTV Operator observes an incident, information will be immediately relayed to the Gwent Police Incident Controller (GPIC) using the dedicated telephone links. The video images will also be passed to GPIC via the video link. The responsible officer in the GPIC will then take the necessary action to ensure the incident receives the appropriate police response; verbal confirmation as to the purpose of the disclosure will be given at this stage.

7.2.3 When in direct contact with the CCTV Control Room, the GPIC officer can request the appropriate type of monitoring from the CCTV Duty Operator. Details and response should be noted in the daily occurrence log.

7.2.4 Close liaison and co-operation is essential at all times. Ultimate control lies with the Council as the System owner.

7.2.5 Should it be necessary for the Police to stay in contact with the Duty Controller for any length of time, contact between Newport City Council and the Police can continue, as a second dedicated direct emergency line is available for reporting any new incidents.

7.3 Secondary Control

7.3.1 No secondary control 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 most senior representative of the System owners, or designated deputy of equal standing. (Owners should make a note of his/her agreement/disagreement to the Police request).

7.4.2 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 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 monitoring room and personal control of all associated equipment, to the 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 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 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 NCC 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.

Section 8 Access to and Security of, Monitoring 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 monitoring room, (or equipment associated with the CCTV System).

8.1.2 The monitoring facility will be staffed when in use; at no time will the facility be left unattended or insecure when equipment is in use.

8.1.3 Care must be taken to ensure all sensitive data such as prints and evidential material are kept secure and out of view.

8.2 Public Access

8.2.1 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.

8.3 Authorised Visits

8.3.1 Visits made 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 monitoring room, including inspectors and auditors, will be required to sign the visitors' book and a declaration of confidentiality.

Note: *A notice at the entrance to the room is placed informing visitors they are entering a restricted area, and entry is dependent upon acceptance of the need for confidentiality. A typical notice is included in Appendix C.*

8.5 Security

8.5.1 Authorised personnel will normally be present at all times when the equipment is in use. (Except for 8.6) If the monitoring 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.

8.5.2 The monitoring room will at all times be secured by 'Magnetic Locks' operated by the CCTV operator

Note: *A fixed view camera is located external to the control room to enable the operator to view visitors before granting entry. Intercom/Door entry system in situ to speak to visitors before granting entry to building.*

8.6 Emergency Evacuation Procedures

8.6.1 On the occasion of the Control Room lying within an emergency evacuation area, CCTV Duty Controllers will be expected to vacate the Control Room and adhere to the Fire Evacuation Procedures.

.

8.6.2 On departure from the CCTV Control Room, the Control Room will be secured against unauthorised entry.

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.

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, DVD 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 monitoring 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 Evidential Recordings

9.2.1 In the event of a recording being required for evidential purposes the procedures outlines in the Procedural Manual will be strictly complied with.

Section 10 Video Prints

10.1 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.

10.2 Video prints contain data and will therefore only be released under the terms of Appendix B to this code of practice, “release of data to third parties”.

10.3 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 and the purpose for which the print was taken.

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

Section 11 Communications

11.1 Dedicated telephone links to the Gwent Police incident control room are provided. These will be used to relay all information on incidents that arise, and to communicate information as the incident continues. In these circumstances, verbal confirmation as the purposes of discloser will be accepted.

11.2 The emergency procedures will be used in appropriate cases to call the Fire Brigade or Ambulance.

In addition, liaison with other units is necessary

11.3 Details are available within the Control Room of points of contact with the following and continuously updated.
Fire and Rescue Services
Ambulance Service
Retail radio ‘Storenet’ schemes
Licence premises ‘Nightnet’ schemes
Bus Stations
Railway Stations
British Transport Police
Gwent Police HQ
Community Safety Wardens
BT Telecommunications
Western Power
CCTV Strategy Partners
Others as necessary

Appendix A1. Key Personnel and Responsibilities

1. **System Owners**

Newport City Council Tel: 01633 656656
Civic Centre
Newport
South Wales
NP20 4UR

Responsibilities:

Newport City Council is the 'owner' of the system. The CCTV system manager will be the single point of reference on behalf of the owners. His/her role will include a responsibility to:

i) Ensure the provision and maintenance of all equipment forming part of the Newport City Council CCTV system in accordance with contractual arrangements, which the owners may from time to time enter into.

ii) Ensure the interests of the owners and other organisations are upheld in accordance with the terms of this Code of Practice.

iii) Agree to any proposed alterations and additions to the system, this Code of Practice and/or the Procedural Manual.

System Management

Newport City Council Tel 01633 656656
The CCTV system manager is responsible for the day-to-day operational management of the system.

Responsibilities:
The CCTV system manager is the 'manager' of the Newport City Council CCTV system.

He/she has delegated authority for data control on behalf of the 'data controller'.
His/her role includes responsibility to:

Maintain day-to-day management of the system and staff;

i) Accept overall responsibility for the system and for ensuring that this Code of Practice and Operational Procedures Manual are fully complied with;
ii) Maintain direct liaison with the owners of the system.
iii) Maintain direct liaison with operating partners.

2. Data Controller

Newport City Council Tel 01633 656656 Responsibility delegated to the: - System Manager

Responsibilities:
(Either alone or jointly with other persons) to determine the purpose for and which and manner in which any personal data are, or are to be processed

3. CCTV Control Room Operator

As named in the CCTV Control Room duty roster

Responsibilities:
As set out within the job description/profile for a Communications Operative

4. System Auditor

Newport City Council Tel: 01633 656656
Chief Internal Auditor or delegated representative.

Responsibilities:

i) For the regular audit of the operation and system and compliance with the Code of Practice and Operational Procedures, which may be in the form of irregular spot checks, to include examination of the control room records, video data records and arrangements by appropriate managers for regular reviews of the content of recorded material.

ii) Complaints relating to the operation or management of the function will be dealt with by line management in the first instance. Unresolved issues will be referred to the Chief Internal Auditor.

5. Systems Inspectors

National Security Inspectorate (NSI) Tel: 01628 637512 nsi@nsi.org.uk

Sentinel House
5 Reform Road
Maidenhead
SL6 8BY

Responsibilities:

i) Independent system inspectors may be called in to undertake periodic inspections of the systems operation and working practices, to ensure the schemes full compliance with BS 7958: 2015 and operational objectives as stated in the systems Code of Practice and Operational Procedures.

iii) Where appropriate make recommendations for improvements.

iv) The inspectors will be permitted to the CCTV monitoring room, without prior notice and to the records held within at any time, providing their presence does not disrupt the operational functions of the room. Their findings will be reported to the systems auditor; all visits will be recorded in the CCTV monitoring room.

Appendix A2 System Stakeholder

There is a whole range of stakeholders in CCTV Systems. As operators in the control of the system, it may be necessary to communicate with any of them.
They include:

i) The Public
ii) The Police
iii) Other Emergency Services
iv) The Local Authority (owners of the system)
v) Other Local Authority departments (various)
vi) Control Room supervisors and manager
vii) Control Room operators
viii) Local business (shops licensed premises etc.)

The Public:
Includes local residents, specific local communities, visitors to the area and motorists. They are interested in how the system assists them in their everyday lives and makes their communities safer but are also concerned that it is ethically and within the law.

The Police:
The CCTV system assists the police in the prevention and detection of crime. It provides reliable evidence to assists them with identifying suspects and mounting prosecutions.

Other Emergency Services:

The Fire Service and Ambulance Service may make use of the system to assist them in locating and dealing with incidents.

The Local Authority:
They are usually the owners of the system. They are interested in making the best use of their substantial investment in terms of equipment, staff and money.

Other Local Authority Departments:
These include Housing, Education, Environmental Health and various other departments, making use of the system to assist them in carrying out their duties efficiently and to ensuring that they are promptly informed about matters requiring their attention (e.g. damage to local authority property, abandoned vehicles, etc.)

Control Room Supervisors and Managers:
They are mainly concerned with the proper operation of the Control Room and the CCTV system. Operating standards reflect on them as Supervisors and Managers.

Control Room Operators:
They are interested in the system operating correctly and efficiently so that employment opportunities continue. They have an interest in the Control Room being a good place to work.

Local Business:
Businesses are interested in how the system improves the environment in which they operate – a safer shopping centre is likely to attract more custom for their shops for instance. Depending on specific business interests, they may well be concerned with how it helps reduce theft and damage or instances of violence and disorder in and around business premises.

The stakeholders fall into two main categories when it comes to their principle concerns. The public and businesses are likely to be primarily concerned with:

i) Safety in public places
ii) Fear of crime
iii) Infringement of Human Rights
iv) Their right to privacy
v) The potential misuse of recorded images
vi) The impact on their general freedoms
vii) Use of system to target/victimise minorities

The local Authorities, as owners of the system, and their managers and supervisors are likely to be primarily concerned with:

i) Their responsibility to reduce crime and disorder
ii) The legal basis for the CCTV system
iii) Adherence of staff to the published operating procedures
iv) Monitoring the practices of staff

v) Storage and security of images
vi) Rules regarding the release of images
vii) Dealing with complaints from the public and requests for information

Appendix B Standard for the release of data to third parties

.

1. General Policy

All requests for the release of data shall be processed in accordance with the Procedural Manual. All such requests shall be channelled through the data controller.

Note: The *data controller* is the person who (either alone or jointly with others) determines the purpose for which and the manner in which any personal data is, or are to be processed.

(In most cases the data controller is likely to be the scheme owners or for a 'partnership' or "subcontractor", both share responsibility).

Day to day responsibility for the Newport City Council System is devolved to the Scheme Manager.

BS 7958:2015 provides additional advice on the criteria for disclosure and this will be followed as part of this process.

2. 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 are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:
i) Police
ii) Statutory authorities with powers to prosecute, (e.g. Customs and Excise; Trading Standards, etc.)
iii) Solicitors
iv) Plaintiffs in civil proceedings
v) Accused persons or defendants in criminal proceedings
vi) Other agencies, (which should be specified in the Code of Practice) according to purpose and legal status

c) Upon receipt from a third party of a bona fide request for the release of data, the data controller shall:
   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. A time limit shall be imposed on such retention, which will be notified at the time of the request.

Note: A time limit could apply providing reasonable notice was issued to the agent, prior to the destruction of the held data, (e.g. a time limit was about to expire).

d) In circumstances outlined at note (3) below, (requests by plaintiffs, accused persons or defendants) the data controller, or nominated representative, shall:
   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 is not to 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 evidential value in respect of civil proceedings or tribunals. In such cases a solicitor, or authorised representative of the tribunal, is 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. A charge may be made for this service to cover costs incurred. 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 data controller shall 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.

(5) The data controller can refuse an individual request to view if insufficient or inaccurate information is provided. A search request should specify reasonable accuracy.

3. 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 data controller shall ensure that:
   i) The request does not contravene, and that compliance with the request would not breach, current relevant legislation (e.g. Data Protection Act 1998, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994, etc.);
   ii) Any legislative requirements have been complied with, (e.g. the requirements of the Data Protection Act 1998);
   iii) Due regard has been taken of ay known case law (current or past) which may be relevant, (e.g. R v Brentwood BC ex p. Peck) and
   iv) The request would pass a test of 'disclosure in the public interest'

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 shall 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.
   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.

Note:

a) '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

b) 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)

4. 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 herself 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 himself only, unless all other individuals who may be identified from the same information have consented to the disclosure'

b) In the event of the data controller 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 data controller 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 actioned;
   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).

5. Process of Disclosure:

a) Verify the accuracy of the request.
b) Replay the data to the requester 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 shall be shown.

d) It must not be possible to identify any other individual from the information being shown, (any such information will be blanked-out, either by means of electronic screening or manual editing on the monitor screen).
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 shall be sent to an editing house for processing prior to being sent to the requester.

Note: The Information Commissioners Code of Practice for CCTV makes specific requirements for the precautions to be taken when images are sent to an editing house for processing.

6. Media disclosure

Set procedures for release of data to a third party should be followed, if the means of editing out other personal data does not exist on-site, measures should include the following:

a) In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' shall be followed. If material is to be released the following procedures shall 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 shall state that the receiver must process the data in a manner prescribed by the data controller, e.g. specific identities/data that must not be revealed.
    iii) It shall require that proof of any 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 shall be considered a contract and signed by both parties.

Note: *In the well-publicised case 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 reassurance 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 future accidental broadcasts.*

Attention *is drawn to the requirements of the Information Commissioners in this respect detailed in the Code of Practice summarised above.*

7. Principles

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

a) Recorded material shall 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 shall 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 is specifically prohibited.

Appendix C Restricted Access Notice

WARNING
RESTRICTED
ACCESS
AREA

Everyone, regardless of status, entering this area is required to complete an entry in the Visitors Book.

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 acknowledge 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 Book is your acceptance of these terms'.

Newport City Council
Chief Executive
Will Godfrey

Appendix D

Declaration of Confidentiality

Example of Declaration of Confidentiality

NEWPORT CITY COUNCIL CCTV SURVEILLANCE SYSTEM

I, …….. am retained by Newport City Council to perform the duty of CCTV Control Room Operator. 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 Newport City Council CCTV System, 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.

I further acknowledge that I have been informed and clearly understand that the communication, either verbally or in writing, to any unauthorised person(s) of any information acquired as a result of my employment with Newport City Council may be an offence against the Official Secrets Act of 1911, Section 2 as amended by the Official Secrets Act of 1989.

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

Witness..... Position .....

Dated this..... day of ..... (month) 20.....

Appendix E Subject Access Request Form

NEWPORT CITY 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. Newport City 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)

Newport City Council CCTV System Rights

Newport City 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: Newport City 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. Newport City 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, photographs and fee to:

The CCTV System Manager
Newport City Council
8 Corn Street
Newport
South Wales
NP20 1DJ

If you have any queries regarding this form, or your application, please ring the CCTV System Manager on Tel. No. 01633 656656

NEWPORT CITY 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

Title (tick box as appropriate)	***Mr***		***Mrs***		***Miss***		***Ms***	
Other title (e.g. Dr, Rev, etc.)								
Surname/family name								
First names								
Maiden name/former name								
Sex (tick box)	***Male***				***Female***			
Height								
Date of Birth								
Place of Birth	***Town***							
	County							

Your Current Home Address (to which we will reply)		
	Post Code	
A telephone number will be helpful in case you need to be contacted	***Tel .No.***	

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

Previous address(es)				
Dates of occupancy	***From:***		***To:***	
Dates of occupancy	***From:***		***To:***	

NEWPORT CITY 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**

DECLARTION (to be signed by the applicant)

The information that I have supplied to 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.

Now – please complete Section 4 and then check the 'CHECK' box (on page 5) <u>before</u> returning the form.

NEWPORT CITY 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		

Day and Date of incident		
Time of incident (to within 20 minutes)	Between AM or PM	And AM or PM
Place incident happened (street name, location i.e. outside of 25, King Street, any town etc.)		
Movements of persons involved in incident		
Brief details of incident including any details of vehicles that were involved		

Colour/description of your upper outer garments at the time		Colour/description of your lower outer garments at the time	

NEWPORT CITY COUNCIL CCTV SURVEILLANCE SYSTEM

Data Protection Act, 1998

Before returning this form	• Have you completed ALL Sections in this form?
	• Have you enclosed TWO identification documents?
Please checks	• Have you signed and dated the form?
	• Have you enclosed the £10.00 (ten pounds) 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: **The CCTV Manager, Newport City 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		*Method of Payment*	
		Receipt No.	
		Documents Returned?	
Member of Staff completing this Section:			
Name		*Location*	
Signature		*Date*	

Appendix F Regulation of Investigatory Powers Act Guiding Principles

Advice and Guidance for Control Room Staff and Police Inspectors in respect of CCTV and the Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 came into force on 2nd October 2001. It relates to surveillance by the Police and other agencies and deals in part with the use of directed covert surveillance. Section 26 of this act sets out what is Directed Surveillance. It defines this type of surveillance as: -
Subject to subsection (6), surveillance is directed for the purposes of this Part if it is **covert** but **not intrusive** and is undertaken-

(a) For the purposes of a specific investigation or a specific operation.
(b) In such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
(c) Otherwise than by way of any immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance.

CCTV being used intrusively will be authorised other than by this section of the RIPA Act. Appropriate guidelines already exist for intrusive surveillance.

The impact for staff in the Police control rooms and CCTV monitoring centres, is that there might be cause to monitor for some time, a person or premises using the cameras. In most cases, this will fall into sub section **C** above, i.e. it will be an immediate response to events or circumstances. In this case, it would not require authorisation unless it were to continue for some time. The code says some hours rather than minutes.

In cases where a pre-planned incident or operation wishes to make use of CCTV for such monitoring, an authority will almost certainly be required.

Slow time requests are authorised by a Superintendent or above.

If an authority is required immediately, an Inspector may do so. The forms in both cases must indicate the reason and should fall within one of the following categories:-

(a) In the interests of national security;
(b) For the purpose of preventing or detecting crime or of preventing disorder;
(c) In the interests of the economic well-being of the United Kingdom;
(d) In the interests of public safety;
(e) For the purpose of protecting public health;
(f) For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or
(g) For any purpose (not falling within paragraphs (a) to (f) which is specified for the purposes of this subsection by an order made by the Secretary of State.

In cases where there is doubt as to whether an authorisation is required or not, it may be prudent to obtain the necessary authority verbally and then in writing by way of the forms.

Any authority given should be recorded appropriately for later reference. This should include the name of the officer authorising.

Examples:

Insp. Authorisation

An example of a request requiring Inspector authorisation might be where a car is found in a car park late at night and known to belong to drug dealers. The officers might task CCTV to watch the vehicle over a period of time to note who goes to and from the vehicle.

Supt Authorisation

Where crime squad officers wish to have a shop premises monitored from the outside, which is suspected of dealing in stolen goods over a period of days.

No Authorisation

Where officers come across a local drug dealer sitting in the town centre/street and wish to have the cameras monitor them, so as not to divulge the observation taking place.

Appendix G1 Civil Liberties

Civil Liberties
Guiding Principles

i) Every CCTV scheme must ensure the principles of civil liberties are not being breached. Fundamentally, it must be shown that:

ii) Individual members of the public are not being harassed, and

iii) No other agency (e.g. the police) is in 'regular' control of Local Authority CCTV coverage;

iv) Camera operators will be mindful of exercising prejudices that may lead to complaints of the scheme being used for purposes other than those for which it is intended. The operators may be required to justify the interest in, or recording of, any particular individual, group of individuals or property at any time by virtue of the scheme or by the scheme managers.

v) The following section has been inserted, as there is now a specific offence under the Sexual Offences Act 2003 in terms of Voyeurism. Failure to properly record the reason why an operator has recorded a sexual act taking place could lead him or her open to investigation under this legislation.

Section 67 of the Sexual Offences act 2003 makes it an offence for a person to observe, for the purpose of his own sexual gratification, another person doing a private act, for instance by looking through a window or peephole at someone having sexual intercourse, where he knows the person observed does not consent to being looked at for this purpose.

Subsection (2) covers a person operating equipment with the intention of enabling another person, for his sexual gratification, to observe a third person, doing a private act, where he knows that the other person does not consent to being so viewed. This would cover, for example, a landlord operating a webcam to allow people on the internet for their sexual gratification to view live images of his tenant getting undressed, if he knew that the tenant did not consent to this.

Subsection (3) covers a person recording another person doing a private act with the intention of looking at the recording for his own sexual gratification, or intending other people to look, for their sexual gratification, at the recording, and where he knows that the other does not consent to the recording of that act with that intention. This would therefore cover the person who secretly films someone masturbating in his/her bedroom to show to others for their sexual gratification. Proof that the intention was the sexual gratification of others could be derived from, for example, the fact that the image was posted on a pornographic website, or in a pornographic magazine. The defendant will be caught by the offence whether or not those looking at the image know that the person filmed did not consent to being filmed with that intention.

Subsection (4) would cover someone who, for example drilled a spy-hole or installed a two-way mirror in a house with the intention of spying on someone for

sexual gratification or allowing others to do so. The defendant would be caught even if the peep-hole or mirror were discovered before it was used.

Section 68 of the Sexual Offences Act 2003 defines 'private act' and 'structure' for the purposes of section 67.
This offence can be committed by a male or female against a male or female.

OFFENCES

67 Voyeurism

67(1) A person commits an offence if –
(a) For the purpose of obtaining sexual gratification, he observes another person doing a private act, and
(b) He knows that the other person does not consent to being observed for his sexual gratification.

67(2) A person commits an offence if-
(a) He operates equipment with the intention of enabling another person to observe, for the purpose of obtaining sexual gratification, a third person (B) doing a private act, and
(b) He knows that B does not consent to his operating equipment with that intention.

67(3) A person commits an offence if-
(a) He records another person (B) doing a private act,
(b) He does so with the intention that he or a third person will, for the purpose of obtaining sexual gratification, look at an image of B doing the act, and
(c) He knows that B does not consent to his recording the act with that intention.

67(4) A person commits an offence if he installs equipment, or constructs or adapts a structure or part of a structure, with the intention of enabling himself or another person to commit an offence under subsection (1).

67(5) Penalty – see below

68 Voyeurism: interpretation

68(1) For the purposes of section 67, a person is doing a private act if the person is in a place, which in the circumstances, would reasonably be expected to provide privacy, and-
(a) The person's genitals, buttocks or breasts are exposed or covered only with underwear,
(b) The person is using a lavatory, or
(c) The person is doing a sexual act that is not of a kind ordinarily done in public.

68(2) In section 67, 'structure' includes a tent, vehicle or vessel or other temporary or movable structure.

Appendix G2.	Human Rights Act

THE HUMAN RIGHTS ACT 1998 (HRA)

Background:

The preamble to the Human Rights Act 1998 (HRA) describes it as 'an Act to give greater effect to the rights and freedoms guaranteed under the European Convention on Human Rights' (the Convention). To understand the HRA you need to know something about the history of the Convention.

The Convention was drafted after the Second World War. British lawyers and civil servants were heavily involved in its drafting. The United Kingdom (UK) signed up to the Convention in 1953 and was one of the first countries to do so. In all, 45 countries have now signed up to the Convention including most of the east European, former communist countries and several countries that were once part of the Soviet Union. The countries that have signed up to the Convention make up the Council of Europe.

The Council of Europe is quite separate from the European Union.

The Human Rights Act was passed by Parliament on 9th November 1998 and came into force on 2nd October 2000. The Act gives 'further effect to the rights and freedoms guaranteed under the European Convention on Human Rights'.

The HRA does not bring any new rights or criminal offences, but the Act does bring existing rights into force as part of UK domestic law, which will enable people in the UK to have cases dealt with in UK courts rather than having to take them to Strasbourg for a ruling as was the case before this Act was passed. The Act also gives public authorities a legal duty to act compatibly with the Convention rights.

There are a total of 18 Articles in Part 1 of the HRA, some which are absolute rights as in 'The Right to Life' and others which are qualified rights as in Articles **8 to 11** below.

Qualified rights are rights that may be interfered with or restricted by the state if the activity threatens national security, public safety or health or to deter or detect crime etc. However these rights can only be restricted if the need for that restriction can be shown to be:

Proportionate	**P**
Legal	**L**
Accountable	**A**
Necessity/Compulsion	**N**
Subsidiarity	**S**

Although the organisations CCTV System will not be responsible for restricting any of the rights contained within the HRA, its Managers will be responsible for challenging any restrictions it is being asked to assist in imposing (through surveillance under RIPA, see

below), by challenging any request it receives by applying **PLANS** to any such restriction and obtaining satisfactory justifications to any such requests.

Note: All 18 Articles in the HRA re important but the Articles, which are considered to have a direct impact on the operation of the organisation's CCTV system, are:-

Article 6: RIGHT TO A FAIR TRIAL

When producing videotape evidence, CCTV Operators must bear in mind that evidence being produced can be used to prove innocence as well as guilt. Although it is a Police responsibility for disclosure of evidence under the PACE Act, Operators must ensure that Police Officers or other enforcement agencies are made aware of all the recorded images used whilst monitoring an incident. It is for the enforcement agencies to decide what is or is not relevant evidence and not the CCTV Operator.

The Operator must, if requested, ensure that all relevant evidence is secured in the 'short term' and that all details concerning the production of any evidence are accurately recorded.

Article 8: RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE

It is recognised that everyone has the right to respect for their private and family life, their home and their correspondence.
Except for the prevention of disorder or crime and for the protection of the rights and freedoms of others. The organisation's CCTV System has been set up with clearly defined aims, which are shown in full in its Code of Practice and Operational Manual.

The System clearly recognises people's 'right to privacy' by ensuring all its Operators are properly trained, that there are clear guidelines in the CCTV Operational Manual and Code of Practice, technical safe guards such as 'no dwell zones' are entered into the CCTV System and that regular audits of the System are carried out.

Although general observation will be maintained within the cameras' arcs of observation (the cameras cover public areas and can see what a member of the public could see with the naked eye, albeit from a different angle), CCTV Operators will not follow individual members of the public except when an offence has been committed or in the judgement of the Operator is about to be committed.

Any images captured by CCTV will be held up to a maximum of 31 days. No CCTV images will be released for the purposes of entertainment.

Article 10: FREEDOM OF EXPRESSION

This article carries with it duties and responsibilities by the people who wish to exercise these freedoms. Therefore CCTV will only monitor such events in the interest of public safety, the prevention of disorder or crime, to protect the rights of others and to assist in enforcing any lawful restrictions placed on any such activity.

Article 11: FREEDOM OF ASSEMBLY AND ASSOCIATION

Everyone has the right to peaceful assembly and freedom of association. CCTV will only monitor these events in the interest of public safety, the prevention of disorder or crime and, the protection of the rights and freedoms of others and to assist in enforcing the lawful restrictions placed on any such event.

Article 14: PROHIBITION OF DISCRIMATION

Most Organisations have very clear policies on discrimination. All CCTV Operators are aware of the organisation's policies. No Operator will monitor an individual because of their sex, race, colour, dress, appearance or monitor individuals by stereo typing them in any way.

All Operators must understand that they have a clear responsibility as the operators of the system to assist the organisation in its duty to uphold the HRA. Operators should do nothing that is likely to breach the HRA. If any Operators find themselves in a position where they are unclear as to how they should respond, they are to contact the CCTV Manager for guidance.

Therefore, to comply with Article 8(1), which relates to the privacy of an individual, and Article 8(2) which gives the exception, a risk/threat assessment must be carried out taking five issues into consideration. Remember any infringement by a public authority of another's rights must be justified. Always consider the following principles enshrined in the mnemonic **P.L.A.N.S:**

Proportionality

Is the level of threat or risk to community safety significant in proportion to the number of cameras used, or even the requirement to have a camera system at all? Is the use of the system commensurate to the seriousness of the risks and offences it is in place to protect from? Are the methods employed to monitor as laid out in the Codes of Practice and Procedures? Actions taken whilst operating the system, must be proportional and fair and able to achieve a balance between the needs of society and the rights of the individual, with reference to the act/problem the system is seeking to stop/prevent/mitigate. Therefore, police action must be fair and achieve a balance between the needs of society and the rights of the individual. You must consider all available different options capable of achieving the objective and select the least intrusive. Don't use a sledgehammer to crack a nut!

Legality

CCTV operators must be fully aware and signed up to the system Code of Practice and Procedures, including matters relating to Human Rights and Data Protection.

Accountability

It must be clear that the monitoring is being carried out for appropriate reasons, and governed by publicly available Codes of Practice and Procedures. All actions must be open to scrutiny and fully recorded/documented. Any alternative options must also be considered

and recorded in logs. You must show what factors influenced your decision, including the reasons for not taking action.

Necessity/Compulsion

Is public space surveillance by CCTV necessary at all, or are there other methods to increase community safety and prevent and detect crime. Is there a likelihood of another offence being committed in this surveillance location? All surveillance carried out must be 'necessary in a democratic society'. The operator must be able to justify any infringement of rights, and record them as such.

Subsidiary

The means of operation of the CCTV system should cause minimum interference with the privacy and the rights of the individual and will be tested and enforced through devolved UK courts.
All these issues need to be fully considered before setting up public place CCTV. However, the Human Rights Act only affects those acting as a public authority. There is no express definition in the Act but they include:

- Government departments
- Local authorities
- Police, prison, immigration officers
- Public prosecutors
- Courts and tribunals
- Non-departmental public bodies (NDPBs)

Any person exercising a public function

As far as 'any person exercising a public function' is concerned it must be understood that this role may vary. So, for example, Group 4 is a public authority in relation to its acts when transporting prisoners, but not when offering security services to a supermarket. In some cases it will be difficult to know if a body is a public authority and if so, into which category it falls. Take legal advice.

CCTV operation is not only affected by the Human Rights Act, but also must conform to the requirements of the Data Protection act 1998. To conduct public space surveillance there must be a legal base in law for operation. CCTV Systems that fall within the jurisdiction of the act are those that are dealing with surveillance in '**areas where the public have largely free and unrestricted access'.** Schemes, which monitor spaces to which the public have access, such as town centres, may be able to rely on Paragraph 5(d) of Schedule 2 of DPA 98 as they are exercising a public function of a nature which is conducted in the public interest. *These purposes include prevention and detection of crime, apprehension and prosecuting of offenders or public/employee safety (Sec 29 DPA 98).*

Schemes, which monitor spaces in shops or retail centres to which the public have access may be able to rely on Paragraph 6(1) of Schedule 2 DPA 98 for their legal basis in law. This is because the CCTV surveillance is necessary for the purposes of the legitimate

interests of the data controller or the third party/ies to whom the data (images) are disclosed. For example; CCTV surveillance is operated 1.' In the substantial public interest' and 2. ' is necessary for the purposes of detection and prevention of crime or any unlawful act'. 'And must be carried out without the explicit consent of the data subject (person) so not to prejudice 1 and/or 2. (Therefore shopping precincts etc. which are not under Police and/or Local Authority surveillance can gather data/images using CCTV, except where the processing is unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the data subject (person).) Signs must advertise the use of CCTV surveillance.

Users of CCTV schemes in town centres, which are run/operated on behalf of the Police or Local Authority (or partnership of the two, both being the Data Controller and taking a dual responsibility for compliance with the DPA) may be able to rely on Paragraph 7(1)(b) Schedule 3 DPA 98 for their legal basis in law. This is because CCTV surveillance is necessary for the exercise of its public function. It may be that the use of such information/images by a public authority in order to meet the objectives of the Crime and Disorder Act 1998 would satisfy this criterion. (Therefore CCTV schemes which are part of a Crime and Disorder Reduction Partnership are permitted. Sec 115 of C&D Act 98 also gives Responsible Authorities the legal basis to exchange data).

Remember the Regulation of Investigator Powers Act 2000 deals with the covert use of surveillance

Human Rights Act Risk Assessment for CCTV Operators	
How have P.L.A.N.S been applied	✓
Have other methods been considered before implementing the use of CCTV	✓
Is the number/location/operation of cameras proportionate to the perceived threats of crime or disorder!	✓
Is the use of the system balanced with the perceived threats!	✓
Are monitoring practices compliant with the laid down rules and procedures!	✓
Are records properly completed and kept to ensure actions can be accounted for!	✓
Is the balance between the rights of the individuals to privacy and rights of others to safety and security set right!	✓
Are the public aware of the rules under which the system operates and are the Code of Practice accessible to them!	✓
Is there an effective complaints procedure in place!	✓
Is CCTV monitoring necessary or could other, less intrusive methods be used!	✓
Is interference with individual's rights the minimum needed to archive the legal purpose!	✓

Appendix H – The guiding principles of the Surveillance Camera Code of Practice.

System operators should adopt the following 12 guiding principles:

- Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
- The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
- There must be as much transparency in the use of surveillance camera system as possible, including a published contact point of access to information and complaints
- There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
- Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
- No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
- Access to retained images and information should be restricted and their must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
- Surveillance camera system operators should consider any operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards
- Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
- There should be effective review and audit mechanism to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
- When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
- Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.