CONWY
CYNGOR BWRDEISTREF SIROL
COUNTY BOROUGH COUNCIL

CONWY COUNTY BOROUGH COUNCIL

CCTV SCHEME

CODE OF PRACTICE

Partneriaeth Diogelwch Cymunedol Conwy
Mewn dwylo diogel
Conwy Community Safety Partnership
In safe hands

Table of Contents.

Acknowledgements / References.

An All Wales CCTV User Group Code of Practice incorporating advice from
Local Government Information Unit (LGIU), the CCTV User Group,
Police Scientific Development Branch, (PSDB) and the Home Office.
And Complying With:
BS7958 Closed Circuit Television (CCTV) – Management and Operation – Code of Practice
BS7499: 2002 Static Site Guarding and Mobile Patrol Services – Code of Practice (Relevant Parts)
BHS7858: 2004 Security Screening of Individuals Employed in a Security Environment – Code of Practice
Data Protection Authority CCTV Code of Practice.

1 GLOSSSARY.

TERM	EXPLANATION
16-"Week Security Screening Period"	The period in which the complete Security Screening Process must be completed.
Ancillary Staff	Staff employed in 'non-relevant' employment.
BS7499: 2002	Code of Practice for Static Guarding, Mobile Patrol and key holding services
BS7858: 2004	Code of Practice for security screening of personnel employed in a security environment
BS7958: 1999	Closed Circuit Television (CCTV) Management and operation – Code of Practice
BS EN ISO 9001	Quality Management Systems – Requirements
CCTV Scheme	Totality of arrangements for closed circuit television in a locality including, but not limited to, the technological system, staff and operational procedures. NOTE: A whole system is not limited to equipment sited at one locality. It may include systems that use dial in dial out, remote transmission or decentralized zone.
CCTV System	Surveillance items comprising cameras and associated equipment for monitoring, transmission and controlling purposes, for use in a defined security zone.
Confirmed Employment	Employment granted upon successful completion of security screening and any additional criteria applied by the organisation.
Control Room	Secure area in a building where CCTV data is monitored. retrieved and analysed.
COSHH	Control of Substances Harmful to Health Regulations 2002
Data	All information including that about a person. NOTE: In CCTV systems, this includes pictures, and any other associated, linked or processed information
Data Controller	A person who determines the purposes for which and in the manner in which any personal data are to be processed or disclosed

Data Processor	A person who processes stored data on behalf of the Data Controller
DDA	Disability Discrimination Act 1995
DPA	Data Protection Act 1998
DSE	Display Screen Equipment Any alphanumeric or graphic screen regardless of the display process involved. Both conventional (cathode ray tube) display screens and other display processes such as liquid crystal displays and other emerging technologies.
Hard Copy Print	Paper copy of an image or images, which already exist on recorded material.
HSW	Health and Safety at Work Act 1974.
Incident	Activity that raises cause for concern that an offence has been, is being, or is about to be, committed, or that an occurrence has taken placed warranting specific action by an operator.
Job Description	A document that details the relevant activities and responsibilities associated with an identified role or position within the organisation.
Manager	Person appointed to supervise and enforce the implementation of the policies and procedures as defined by the owner of the scheme.
Observation Mode	Mode of operation of a CCTV system, whereby monitoring is carried out live, the sole purpose of which is to observe an operation in its real time and not to record, hold in memory, or print the information received.
Operator	Person specifically designated and authorized by the owner of a CCTV system to carry out the physical operation of controlling that system. NOTE: The meaning of the word 'operator' in the setting of The Health and Safety (Display Screen Equipment) Regulations 1992 is different to the use of the word at other parts of this document.

Owner	Legal person or entity, agency or individual designated as having overall responsibility for the formulation and implementation of the policies, purposes and control of a CCTV scheme. NOTE: The Role of Owner also includes all statutory responsibilities, including the role of 'data controller' as prescribed by D P A, 1998, section 1, subsection 1[1]. The owner may be a partnership, provided it has a formal constitution.
Particulars of Employment	A document containing the various details pertaining to a new member of staff's employment including start date, job title, location, hours of work, remuneration, etc.
Partner	Individuals or groups who jointly have responsibility for the establishment of an organisation and its ongoing management and operation each party having equal responsibility, usually under the control of an elected executive officer.
Personal Data	'Data which relate to a living individual who can be identified: from those data, or f*rom those data and other information which is in the possession of, or is likely to come into the possession of, the data controller'.*
Processing	'In relation to information or data, means obtaining, processing, recording or holding the information or data or carrying out any operation or set of operations on the information or data.
Provisional Employment	Initial period of employment for a new individual after completion of initial security screening and during which full security screening will be completed.
Recorded Material	Any data recorded on any medium that has the capacity to store data can later be recalled irrespective of time.
Recording Material	Any medium that has the capacity to store data and from which data can later be recalled irrespective of time.
Relevant Employment	A person who, on whatever basis, is employed within the private security environment.
Retrieval System	CCTV system having the capability, in any medium, of effectively capturing data that can later be retrieved, viewed or processed.

RIPA	Regulation of Investigatory Powers Act 2000
Screening Controller	Individual within an organisation responsible for management of screening.
Security Screening Period	Period of not less than 10 years immediately prior to the commencement of relevant employment or transfer to relevant employment, or back to the date of ceasing full-time secondary education, if this date is more recent.
Security Screening Process	An investigative process that is intended to indicate the integrity and suitability of an applicant for employment within a security environment.
Sensitive Personal Data	Personal data stored within a retrieval system that is sensitive by virtue of its contents and implications i.e. data indicating the commission or alleged commission of any offences.
Subject Data	Images being viewed on screen whether directly from a camera or from a tape recording.
Supervisor	Person specifically designated, trained and authorized by the owner of a scheme to ensure that at all times the system is operated in accordance with the code of practice and any procedural instruction issued by the owner or manager. NOTE: This may include the role and responsibilities of "data controller" (See the NOTE in the **Owner** section of this Glossary.)
User	An employee who habitually uses display screen as a significant part of his normal work.
Workstation	A position established and equipped for the purpose of providing a suitable environment for an employee to carry out the duties associated with his/her employment.

2. FOREWORD.

This Code of Practice is intended to be used in conjunction with the detailed Procedural Manual drafted for use by the Conwy County Borough Council CCTV Scheme. ***The procedural Manual is restricted to those involved in the operation and management of the CCTV scheme***.

These documents along with a commitment to staff training are designed to ensure the CCTV system remains effective and is operated to a high standard of integrity and accountability.

The Common Code of Practice will be periodically updated to reflect legislation and recent best practice guidance.

3. STATEMENT OF UNDERTAKING.

Statement of Undertaking.

Code of Practice in Respect of the Operation of the Conwy County Borough Council CCTV System

Agreed by:

Conwy County Borough Council

and North Wales Police.

The content of this Code of Practice and the Procedural Manual are hereby approved in respect of the Conwy County Borough Council Closed Circuit Television System and, as far as is reasonably practicable will be complied with by all who are involved in the management and operation of the System.

Signed for and on behalf of Conwy County Borough Council and North Wales Police.

.....B. Davies,
Chief Executive,
Conwy County Borough Council.

.....J.M Robin,
Chief Constable,
North Wales Police.

Dated.....2010.

NOTE:
This document updates and supersedes the original Code of Practice agreed between Colwyn Borough Council and North Wales Police dated 19th December 1995.

4. INTRODUCTION AND OBJECTIVES.

4.1 INTRODUCTION:

4.1.1 A closed circuit television (CCTV) Scheme that received, holds or processes data about an identified person is obliged to conform to certain legislation, most importantly the Data Protection Act, 1998 (DPA), the Human Rights Act, 1998 (HRA) and latterly, by virtue of registration with N.S.I. under its Silver Scheme, conformance with the relevant British Standards BS 7958: 1999 and BS7858: 2004. This Code of Practice is designed to supplement that legislation in a model code that ensures fairness, purpose and accountability.

4.1.2 The CCTV System has evolved from the formation of a non-executive partnership between North Wales Police and Conwy County Borough Council. For the purpose of this document, the 'Owner' of the system is Conwy County Borough Council and the 'Manager' and therefore 'Data Controller' is the Head of Regulatory Services. Details of key personnel responsibilities and contact points are shown at **Appendix A – Key Personnel and Responsibilities** to this Code.

4.1.3 This Code of Practice (or 'the Code') will be supplemented by a separate Procedural Manual which stipulates instructions on all aspects of the operation of the System. To ensure the purpose and principles (see **Paragraph 5 – Statement of Purpose and Principles**) of the CCTV System are realised, the manual is based upon the principles of this Code of Practice. This Code of Practice has been agreed between those agencies and organisations involved in the development and operation of CCTV schemes within the County Borough of Conwy, namely Conwy County Borough Council and North Wales Police. It is accepted as binding. The principles of this Code will also apply to any other law enforcement agency who wishes to obtain video evidence.

4.1.4 This Code of Practice gives recommendations for the operation and management of CCTV within a controlled environment, where data

that may be offered as evidence is received, stored, reviewed or analysed.

4.1.5 This code of practice is applicable to a CCTV scheme used in public places, which are areas where the public are encouraged to enter or have a right to visit, such as town centres, shopping malls, public transport, health, etc. and overlook a public place.

4.1.6 The purpose of the scheme is to provide a safe environment for those who live, trade, visit and work in the area. This Code is applicable to any CCTV system owned and operated by Conwy County Borough Council and is used in areas where the public have a "*right to visit*". These areas include:

a) a place that is in private ownership, but where the public perceive no boundary
b) a place where public service is offered
c) public footpaths, roads, bridleways, etc
d) educational establishments, hospitals
e) sport grounds, supermarkets, housing areas.

4.2 SCHEME OBJECTIVES:

4.2.1. The main objectives of the CCTV are summarised as:

a) Assist in the detection, prevention and fear of crime,
b) Facilitate the apprehension and prosecution of offenders in relation to crime and public order,
a) Provide residents, visitors and businesses with a greater feeling of safety and security,
b) To enhance community safety, boost the economy and encourage greater use of the town centre/shopping mall, etc.,
c) To assist the Local Authority in its enforcement and regulatory function,
d) To assist with traffic management,

4.2.2 Visual intrusion into dwellings and private office accommodation will be prevented as far as possible, in order to preserve privacy and to ensure that the Scheme is not brought into disrepute.

4.2.3 Conwy County Borough Council and the North Wales Police respect the individual citizen right to privacy. Every effort has been made during the design and installation of all CCTV Schemes to protect this principle as far as practicably possible. If any individual is able to substantiate a reasonable claim that his/her privacy has in some way been infringed, then the matter will be considered by the Council's Complaints Procedure (also refer to **Paragraph 5.2 – Complaints Management**).

4.2.4 The CCTV System is the property of Conwy County Borough Council and the operation is under the direct management control of the Head of Regulatory Services of Conwy County Borough Council who reports to the Council.

4.2.5 Camera locations within the County of Conwy are listed in **Appendix I – Camera Positions/Addressing No's.**

4.2.6 It is recognised that in the partnership between the Council and North Wales Police, it is the function of the Scheme to obtain evidential data relative to incidents within the stated objectives and the function of the Police to apprehend/arrest offenders, as it is the responsibility of the Police to process evidence for prosecution purposes.

4.2.7 The System will be staffed 24 hours each day, 365 days of the year. The Head of Regulatory services Services will manage the system and will retain the discretion of monitoring the System according to circumstances prevailing at the time. Employees of Conwy County Borough Council will staff the Control Room.

4.2.8 Conwy County Borough Council recognises the importance of achieving good quality visual evidence, which may be of use in securing a conviction for a criminal offence. The responsibility for achieving such a conviction lies with the Crown Prosecution Service. Whilst every effort will be made to ensure that the operation of the CCTV Scheme is

beyond reproach, it is clearly the responsibility of North Wales Police to ensure the authenticity of any evidence once handed over from the Control Room and for the eventual return of such evidence to Conwy County Borough Council.

4.3 REVIEW OF CODE OF PRACTICE AND ANNUAL REPORT:

4.3.1 Conwy County Borough Council (Scheme Owner) and North Wales Police recognize the importance of public confidence in this CCTV Scheme. The Code has been drawn up following extensive consultation. The Council and the Police will continue to evaluate the effectiveness of CCTV and the operation of the Code. The Scheme Owners will, carry out an annual review. During its annual review of the Scheme and the formulation and dissemination of an annual report for benefit of the Data Commissioner, review and if required amend this Code.

4.3.3 Such a review will be conducted by the Scheme Owners together with the Data Controller and the Scheme Manager in order to ensure the effectiveness of the system. Only in conjunction with the Scheme Owners can any significant changes be made to the Code of Practice. Changes of a minor nature can be made by the Scheme Manager; however they will be subject to retrospective ratification at the next management meeting and will only be categorised as permanent and formal amendments only when confirmed during the next annual review.

4.3.4 The outputs of the annual review will be Minuted and any agreed action points will be allocated time controlled.

4.3.5 The annual review will precede the compilation of an annual report for information of the Data Commissioner and to be made available within the public domain upon specific request.

4.3.6 The annual report will include, but not be limited to the following topics:

a) A description of the Scheme and the geographic boundaries of operation
b) The Scheme's policy statement
c) The purpose and scope of the Scheme
d) Any changes to the operation or management of the Scheme
e) Any changes to the policy
f) Any proposals to expand or reduce the Scheme either in its boundaries or numbers of cameras
g) The aims and objectives for the next review period
h) Achievements of the Scheme during the past review period, including- (a) Number of incidents recorded and (b) Number of incidents reported to police or other prosecuting agency
i) An assessment of the impact of the Scheme upon crime and public disorder within the Scheme boundaries.

5. STATEMENT OF PURPOSE AND PRINCIPLES.

5.1 GENERAL PRINCIPLES:

5.1.1 The purpose of providing CCTV is to deter the incidence of crime against people and property, improve the prospects of detecting crime, prosecuting offenders, enhancing public safety and confidence by reducing the fear of criminal and anti-social behavior. In addition, it may be used for other Town Centre Management and regulatory services services at the discretion of Conwy Community Safety provided such usage is compatible to the stated objectives of the Scheme.

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

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

5.1.4 The public interest in the operation of the Scheme will be recognized by ensuring the security and integrity of operation procedures.

5.1.5 Throughout this Code of Practice it is intended, as far as reasonably possible; to offer a balance between the objectives of the CCTV Scheme and the need to safeguard the individual's right to privacy. Throughout the Code every effort has been made to indicate that, a formal structure has been put in place, (including a complaints procedure) by which it should be identified that the Scheme is not only accountable, but is seen to be accountable.

5.1.6 Participation in the Scheme by any local organization, 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.

5.2 COMPLAINTS MANAGEMENT:

The Scheme Owners have approved a complaints policy, contained in **Appendix K – Complaints Policy**, which is intended to ensure that any complaint, real or perceived is dealt with quickly and with impartiality. Any complaint received by the Scheme will be passed directly to the Scheme Manager in order to ensure a prompt appropriate response. The procedure for management of complaints is contained in **Section 18 of the Procedures Manual.**

5.3 COPYRIGHT:

Copyright and ownership of all material recorded by virtue of the Conwy County Borough Council CCTV System will remain with the Data Controller.

5.4 CAMERAS AND AREA COVERAGE:

5.4.1. Geographical areas covered by the Scheme:

Abergele
Colwyn Bay
Conwy
Deganwy
Glan Conwy
Kinmel Bay
Llandudno Junction
Llandudno
Llysfaen
Mochdre
Old Colwyn
Penmaenmawr
Rhos on Sea
Towyn
Camera locations listed in Appendix 1.

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

5.4.3 Monochrome cameras and/or the use of infra red illumination lamps may be employed if lighting/operational conditions dictate.

5.4.4 Covert cameras will not be employed.

5.4.5 Audio recording of public areas will not take place.

5.4.6 Privacy "zoning" will be employed where visual intrusion of private dwellings is likely.

5.5 MONITORING FACILITIES:

5.5.1 A staffed monitoring room is located within the County Borough area.

5.5.2 Secondary monitoring equipment is located within the North Wales Police control room and monitoring centre. However no equipment, other than that housed within the main CCTV control room has the capability to record images from any of the cameras.

5.5.3 At least one operator will be present within the Control Room throughout operation hours. Continuous camera surveillance will be maintained throughout.

5.5.4 At ALL times the control of the system will remain with Conwy County Borough Council.

5.5.5 In the event of North Wales Police or any law enforcement agency requiring or wishing an Officer to undertake monitoring in the main CCTV control room, this will normally be allows subject to permission by the CCTV Scheme Manager and appropriate authorisation in respect of RIPA is in place. All such events will be logged.

5.6 RECORDING FACILITIES:

5.6.1 Pictures relayed from every camera will be recorded. All recordings will be "overwritten" (erased) on a 31 day cycle.

5.6.2 There will be facilities available to transfer images to removable media. All transfers of images will be noted and logged.

5.6.3 ALL recordings of signals from this system remain the property of Conwy County Borough Council. No recordings are to be shown, lent, hired, sold or advised to ANY unauthorised party.

5.6.4 Any removable media containing video images transferred / copied from the System will have an Unique Reference Number and noted in system records.

5.6.5 In the event of any removable media being created which contain images for evidential use they will be stored in the CCTV control room for 28 days before destruction.

5.6.6 Any images, including “stills”, stored within the control room will be periodically reviewed and destroyed by the Scheme Manager.

5.6.7 Conwy County Borough Council will ensure that all information containing criminal evidence will only be handed to the Police or other prosecuting agency if the operator is satisfied that the nature of the evidence warrants such action.

5.6.15 The Data Controller is authorised to release images into the public domain, provided the action is considered to conform to the objectives of the Scheme listed in **Paragraph 4.2 – Scheme Objectives**.

5.7 EVIDENTIAL INFORMATION:

5.7.1 To ensure that data, whatever format, can be used in evidence, the following procedures will be followed:

The operator will register, through the CCTV Management Information System:

a) the date and time of any incident,

b) The date and time of creating any removable media evidence,

c) Relevant information regarding the incident,

d) Any law enforcement agency involvement.

5.7.2 Incident recordings will be retained for twenty eight days from recording prior to being erased or destroyed. It is recognised that it is the responsibility of North Wales Police to inform the CCTV Control Room if recorded evidence is required for evidential purposes and collect any such evidence within the 28 day period.

5.7.3 A record will be maintained on a register of the release of recorded evidence to the Police or to other authorised applicants.

5.7.4 In the event of an incident recorded on video tape being required for the defence of an individual, all conditions appertaining to release of tapes to the Police will also apply.

5.7.5 All recording medium not signed out must remain within the CCTV Control Room

5.7.6 It is the responsibility of the recipient of any images obtained from the Control Room to either return the medium or confirm its destruction.

5.8 PHOTOGRAPHS:

5.8.1 Any image extracted from the system shall only be used to assist in achieving and maintaining the objectives of the system.

5.8.2 Any issue of hard copy images from the CCTV system will be noted.

5.8.3 A file of photographs (still images) may be maintained showing appropriate cross-references to recordings.

5.9 OPERATORS INSTRUCTIONS:

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

6 PRIVACY AND DATA PROTECTION.

6.1 PUBLIC CONCERN:

6.1.1 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.

NB: 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:

a) organisation, adaption or alteration of the information or data

b) retrieval, consultation or use of the information or data

c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

d) alignment, combination, blocking, erasure or destruction of the information or data.

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

6.2 DATA PROTECTION LEGISLATION:

6.2.1 The Conwy county Borough Council CCTV System is registered with the office of the Data Protection Commissioner with the Head of Regulatory Services being nominated as Data Controller.

6.2.2 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:

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

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

c) Personal data will be used only for the purposes, and disclosed only to the people, shown within these codes of practice.

d) Only personal data will be held which are adequate, relevant and not excessive

e) in relation to the purpose for which the data are held.

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

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

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

i) Procedures will be implemented to put in place security measures to prevent:

   i. unauthorised or accidental access to, alteration, disclosure or loss and

   ii. destruction of, information.

6.3 REQUEST FOR INFORMATION (Subject Access):

6.3.2 Any request from an individual for the disclosure of personal data which he/she believes is recorded by virtue of the system will be directed to the System Manager, (or Data Controller).

6.3.3 The principles of Sections 7 and 8 of the Data Protection Act 1998 (Rights of Data Subjects and Others) should be followed in respect of every request; those Sections are reproduced as **Appendix B – Extracts from the Data Protection Act, 1998) to these codes.**

6.4 EXEMPTIONS TO THE PROVISION OF INFORMATION:

6.4.1 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.

1. Personal data processed for any of the following purposes –

a) the prevention or detection of crime

b) the apprehension or prosecution of offenders.

are exempt from the subject access provision 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'.

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

6.5 CRIMINAL PROCEDURES AND INVESTIGATIONS ACT, 1996:

6.5.1 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). Any 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).

7. ACCOUNTABILITY AND PUBLIC INFORMATION.

7.1.1 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.

7.1.2 Cameras will not be used to look into private residential property. 'Privacy zones' may 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.

7.1.3 A member of the public wishing to register a complaint with regard to any aspect of the Conwy County Borough Council CCTV System may do so by contacting the Chief Executive of the Authority or the Head of Regulatory Services office. Any complaint will be dealt with in accordance with existing rules and regulations to which all members of Conwy County Borough Council, including the CCTV operators, are subject.

7.1.4 Conwy County Borough Council, being the Scheme Owners,

a) will receive regular and frequent reports from the manager of the Scheme

b) may nominate a committee with a specific responsibility for receiving and considering those reports.

c) Formal consultation will take place between the owners and the managers of the Scheme with regard to all aspects of the Scheme.

7.1.5 The nominated Scheme Manager named at will have day-to-day responsibility for the Scheme as a whole.

7.1.6 The Scheme will be audited by Conwy County Borough Council, (or nominated deputy whose organisational level of responsibility is at

least equal to that of the Scheme Manager, but not the Scheme Manager.

7.1.7 Statistical and other relevant information, including any complaints made, will be included in the Annual Report of Conwy County Borough Council which will be made publicly available.

7.1.8 A public information leaflet (see **Appendix M – Public Information Leaflet**); will be made available to anyone requesting them. Additional copies will be lodged at libraries, Town and Community Councils within the County of Conwy and main offices of Conwy County Borough Council.

7.1.9 Annual Report: A copy of the annual report will also be made available to anyone requesting it. Additional copies will be lodged at public libraries, Town and Community Councils within the County of Conwy and main offices of Conwy County Borough Council.

7.1.10 Signs: Signs will be placed in the locality of the cameras and at the main entrance points to the relevant areas, e.g. Railway and Bus stations. The signs will indicate:

a) The presence of CCTV monitoring,

b) The 'ownership' of the system, i.e. Conwy County Borough Council, and

c) Contact telephone number of the 'Data Controller' of the system.

8 ASSESSMENT OF THE SYSTEM AND CODE OF PRACTICE.

8.1 MONITORING:

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

8.2 AUDIT:

The Scheme Owners will ensure that persons not directly involved with day to day management and operational issues will be responsible for regularly auditing the operation of the Scheme 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, video tape histories and the content of recorded material.

The audit function has additionally been outsourced for external verification to the National Security Inspectorate who will conduct regular audits in compliance with their audit protocol.

9 HUMAN RESORUCES.

9.1 OWNERSHIP:

The CCTV Scheme is owned by the Conwy County Borough Council under the direct control of the Head of Regulatory services Services.

9.2 STAFFING OF THE MONITORING ROOM:

9.2.1 The CCTV Monitoring Room will be staffed in accordance with internal procedures. Equipment associated with the CCTV System will only be operated by authorised personnel who will have been properly trained in its use and all monitoring room procedures. Each operator will have access to, or be personally issued with a copy of both the codes of practice and procedural manual. They will be fully conversant with the contents of both documents, which may be updated from time to time, and which he/she will be expected to comply with as far as is reasonably practicable at all times. Failure by staff to comply with Codes of Practice or Procedural Manuals will be considered a severe breach of discipline and may result in disciplinary, civil or in certain circumstances criminal prosecution.

9.2.2 All staff recruited will be thoroughly checked and vetted in accordance with local authority procedures and in compliance with BS 7499: 2002 and BS 7858 2004 to ensure that only people of suitable calibre and integrity are employed to monitor and operate CCTV Scheme. Completion of a suitable probationary period will be subject to validation of security checks, employment, health and other details.

9.2.3 Every individual who is involved with the CCTV system in terms of this Code of Practice will be required to sign a declaration of confidentiality.

UNDER NO CIRCUMSTANCES WILL UNTRAINED STAFF USE THE SYSTEM

9.3 TRAINING:

9.3.1 The success and effectiveness of the CCTV Scheme will largely depend upon its trained operators. The owners of the Scheme will ensure that all its staff are fully trained to the standard required by BS 7958: 1999 and in compliance with guidelines issued by them so that maximum benefit is derived from the Scheme and a mutual understanding of working practices achieved.

Training will include:

a) Working conditions, including terms of employment and H&S issues

b) The use of appropriate equipment

c) The operation of appropriate systems, including local knowledge of sites to be monitored

d) Management of recorded material, including handling and storage of data

e) Relevant legislation and legal issues

f) Privacy and disclosure issues

g) Discipline Policy.

9.3.2 Such training will be delivered in a combination of off site classroom training and on site structured training and evaluation.

9.3.3 Both external and internal training will be evaluated with the trainees through personal interview with the Scheme Manager and completion of a training evaluation record.

9.3.4 Additional training needs for remedial purposes or for career development to a nationally recognised qualification will be evaluated on a minimum 12 monthly basis through annual appraisal.

9.4 DISCIPLINE:

9.4.1 Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with the CCTV Scheme to which they refer, will be subject to Conwy County Borough Council discipline code. Any breach of this Code of Practice or of any aspect of

confidentiality will be dealt with in accordance with those discipline rules.

9.4.2 The Scheme Manager will accept primary responsibility for ensuring there is no breach of security and that the Code of Practice is complied with. He/she has day to day responsibility for the management of the control room and for enforcing the discipline rules.

9.5 DECLARATION OF CONFIDENTIALITY:

9.5.1 Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with the CCTV System to which they refer, will be required to sign a declaration of confidentiality. This includes staff and Contractors.

9.5.2 Every visitor to the control room will be required to sign in the visitor's book, in doing so they are signing a declaration of confidentiality appended thereto.

9.5.3 All Contractors and subcontractors visiting the control room for any installation or maintenance function will sign a declaration of confidentiality prior to accessing the control room. **Appendix F – Contractors Declaration of Confidentiality**, (see also **Paragraph 11.1 Condition of Access**, concerning access to the monitoring room by others).

10 CONTROL AND OPERATION OF CAMERAS.

10.1 GUIDING PRINCIPLES:

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

10.1.2 Every use of the cameras will accord with the purposes and key objectives of the Scheme and shall be in compliance with this Code of Practice.

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

10.1.4 Camera operators will be mindful of exercising prejudices which 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 their interest in, or recording of, any particular individual, group of individuals or property at any time by virtue of the audit of the Scheme or by the System Manager.

10.1.5 Random audit will be undertaken by the Scheme Manager/Supervisor to ensure that all stored data has been captured in pursuance of the defined objectives of the Scheme and that the principles of the Scheme are not compromised. All random audits will be documented to include time/date of audit, data audited and outcome.

10.1.6 Should any Member of the Public have concerns that any camera within the system may unnecessary infringe upon their privacy they may contact the Scheme Manager who, will, if satisfied, the request is bone fine resolve the problem. If the complainant is not satisfied of this response, a further complaint will be considered in accordance with the Council's Complaints Procedure.

10.2 PRIMARY CONTROL:

Only CCTV Operators and the CCTV Scheme Manager will have access to the operating controls.

10.3 SECONDARY CONTROL:

Secondary control will not take place.

10.4 INCIDENT PROTOCOL:

10.4.1 In the event of an incident being seen by a CCTV Operator, which he/she considers should require action he/she must note the incident and contact the appropriate emergency service or LA department. The Operator must contact the police if he./she observe a criminal act taking place or a person(s) acting in a suspicious manner.

10.4.2 An incident can be defined as:

(a) A circumstance, or set of circumstances that give rise to belief than an offence or public disorder situation is in progress, is about to occur or has just occurred and that the objectives of The Scheme, (prevention, detection of crime, identification of offenders or restoration of public tranquillity) can be advanced by directed surveillance.

Or

(b) In the case of the maintenance of free flow of traffic, identification of the cause of interruption in traffic flow which, by direct intervention, can be better managed or reduced.

(c) In circumstances where a person or persons are identified in circumstances that may be considered to render them vulnerable.

10.4.3 The CCTV Operator must complete the Incident Report for any observed incident. All incidents will be logged by the CCTV Operator.

10.4.5 Direct surveillance will only be maintained for as long as is necessary to observe the restoration of normality or until all data necessary to provide evidence to support a subsequent prosecution has been obtained.

11 ACCESS TO, AND SECURITY OF, MONITORING ROOM AND/OR ASSOCIATED EQUIPMENT.

11.1 CONDITION OF ACCESS:

11.1.1 The Control Room door will be security locked at all times.

11.1.2 Access to the Control Room will be strictly limited to those listed in **Appendix J – CCTV Control Room Access.**

11.1.3 Regardless of their status, all visitors to the CCTV monitoring room, including inspectors and auditors, will be required to sign the visitor's book and the declaration of confidentiality.

11.2 SECURITY:

Authorised personnel will normally be present at all times when the equipment is in use. If the monitoring facility is to be left unattended due to an emergency situation it will be secured. In the event of the monitoring room having been evacuated for safety or security reasons, the provision of the Procedural Manual will be complied with.

12. MANAGEMENT OF RECORDED MATERIAL.

12.1 GUIDING PRINCIPLES:

12.1.1 For the purposes of this Code 'recorded material' means any material recorded by, or as a result of, technical equipment which forms part of the Conwy County Borough Council Closed Circuit Television System, but specifically includes images recorded digitally, or on videotape or by way of video copying, including video prints.

12.1.2 Every video recording used in conjunction with the Conwy County Borough Council CCTV System has the potential of containing material that has been admitted in evidence at some point during its life span.

12.1.3 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.

12.1.4 It is therefore of the utmost importance that every means (e.g. tape/CD/DVD/memory device) of video recording is treated strictly in accordance with this Code of Practice and the Procedural Manual from the moment it is delivered to the monitoring room until its final destruction. Every movement and usage will be meticulously recorded.

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

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

12.2 NATIONAL STANDARD FOR THE RELEASE OF DATA TO A THIRD PARTY:

12.2.1 Every request for the release of personal data generated by this CCTV Scheme will be channelled through the Scheme Manager (or Data Controller). The Scheme Manager will ensure the principles contained within **Appendix C – National Standard for the Release of Data to Third Parties**) to this Code of Practice are followed at all times.

12.2.2 In complying with the national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's 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 this Code of Practice;

b) Access to recorded material will only take place in accordance with the standards outlined in **Appendix C – National Standard for the Release of Data to Third Parties** and this Code of Practice;

c) The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

12.2.3 Members of the police service or other agency having a statutory authority to investigate and/or prosecute offences may, subject to compliance with **Appendix C – National Standard For the Release of Data to Third Parties**, release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses. Under such circumstances full details will be recorded in accordance with the Procedural Manual. **Note**: Release to the media of recorded information, in whatever format, which may be part of a current investigation would be covered by the Police and Criminal Evidence Act, 1984. Any such disclosure should only be made after due consideration of the likely impact on a criminal trial. Full details of any media coverage must be recorded and brought to the attention of both the prosecutor and the defence.

12.2.4 If material is shown to witnesses, including police officers, for the purpose of obtaining identification evidence, it must be shown in accordance with **Appendix C – National Standard for the Release of Data to Third Parties** and the Procedural Manual.

12.2.5 It may be beneficial to make use of 'real' video footage for the training and education of those involved in the operation and management of CCTV systems, and for those involved in the investigation, prevention

and detection of crime. Any material recorded by virtue of this CCTV system will only be used for such bona fide training and education purposes.

12.3 VIDEO TAPES AND OTHER RECORDING MEDIA – PROVISION & QUALITY:

To ensure the quality of the images and that recorded information will meet the criteria outlined by current Home Office guidelines, only recordable media meant for the process will be used.

12.4 RECORDED MEDIA – RETENTION:

12.4.1 Recorded media, which contain real time recorded data will be retained for a period of 28 days.

12.4.2 Hard drive recorders are not suitable for removing. If the whole data contained on such a medium is required for investigative use then a direct copy image must be carried out.

12.5 RECORDED MEDIUM REGISTER:

Each recording medium will have a unique tracking record. The records which will be retained for at least three years, after the medium has been destroyed.

12.6 RECORDING POLICY:

All camera images are recorded by the system. Images are overwritten and therefore destroyed on a 31 day cycle. Operators have the facility to create another file image which may be stored in the control room or on a removable media. The Scheme Manager will ensure a regular audit of all such images.

12.7 EVIDENTIAL MATERIAL FOR POLICE USE:

12.7.1 It is the responsibility of the Police to manage the gathering of video recorded evidence to aid the prosecution of offenders, retention of that

material until the case, or until the expiry of statutory time limits allowed for appeal.

12.7.2 Each media will have a unique reference number. All recorded media used in the Scheme shall be catalogued in an appropriate register. It is the responsibility of the Police or other appropriate agency who have access to video evidence to return the medium to the control room or confirm its destruction.

13 APPENDIX A – KEY PERSONNEL AND RESPONSIBILITIES.

13.1 OWNERSHIP:

The Owner of the Scheme is:

Conwy County Borough Council
Civic Centre, Bodlondeb, Conwy
Tel: 01492 – 575400

13.2 OWNERS RESPONSIBILITIES:

Conwy County Borough Council nominates a single point of reference as Manager and Data Controller of the System whom is the Head of Regulatory Services.

13.3 MANAGER/DATA CONTROLLER RESPONSIBILITIES:

The Manager and Data Controller of the System is:
Head of Regulatory Services, Civic Offices, Colwyn Bay. LL29 8AR.
Tel: 01492 – 575203.
The Head of Regulatory Services is responsible:

a) to the Owner of the CCTV System,
b) responsible for nominating a Scheme Manager,
c) ensuring that the interests of Conwy County Borough Council are upheld in accordance with the terms of this Code of Practice,
d) ensuring the Owners are kept up to date as to the performance of the System and changes or amendments to the Code of Practice.

13.4 SCHEME MANAGER RESPONSIBILITIES:

The Manager of the System is responsible for ensuring that the System is managed by a Scheme Manager.
His / Her role will include a responsibility to:

a) Maintain day to day management of the system and staff;

b) Accept overall responsibility for the system and for ensuring that this Code of Practice is complied with;

c) Ensure that every Operator will operate the System in accordance with the Code of Practice and Procedural Manual.

d) Maintain close liaison with the Manger and Data Controller of the system.

14 APPENDIX B – EXTRACTS FROM THE DATA PROTECTION ACT, 1998.

Section 7

1) Subject to the following provisions of this section and to sections 8 and 9, an individual is entitled:

a) To be informed by any Data Controller whether personal data of which that individual is the data subject are being processed by or on behalf of that Data Controller,

b) If that is the case, to be given by the Data Controller a description of:
   i) the personal data of which that individual is the data subject;
   ii) the purpose for which they are being or are to be processed;
   iii) the recipients or classes of recipients to whom they are or may be disclosed,

c) To have communicated to him/her in an intelligible form:
   i) the information constituting any personal data of which that individual is the data subject, and
   ii) any information available to the Data Controller as the source of those data and

d) where the processing by automatic means of personal data of which that individual is the data subject for the purposes of evaluating matters relating to him/her such as, for example, his/her performance at work, his/her creditworthiness, his/her reliability or his/her conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him/her, to be informed by the Data Controller of the logic involved in that decision-taking.

2) A Data Controller is not obliged to supply any information under subsection (1) unless he/she has received:

a) a request in writing, and

b) except in prescribed cases, such fee (not exceeding the prescribed maximum) as he/she may require.

3) A Data Controller is not obliged to comply with a request under this section unless he/she is supplied with such information as he/she may reasonably require in order to satisfy him/herself as to the identity of the person making the request and to locate the information which that person seeks.

4) Where a Data Controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he/she is not obliged to comply with the request unless: (a) the other individual has consented to the disclosure of the information to the person making the request, or (b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

5) In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request; and that subsection is not be construed as excusing the Data Controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by omission of names or other identifying particulars or otherwise.

6) In determining for the purposes of subsection (4)(b) whether it is reasonable in all circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular, to:

a) any duty of confidentiality owed to the other individual,
b) any steps taken by the Data Controller with a view to seeking the consent of the other individual,
c) whether the other individual is capable of giving consent, and
d) any express refusal of consent by the other individual.

7) An individual making a request under this section may, in such cases as may be prescribed, specify that his/her request is limited to personal data of any prescribed description.

8) Subject to subsection (4), a Data Controller shall comply with a request under this section promptly and in any event before the end of the prescribed period beginning with the relevant day.

9) If a court is satisfied on the application of any person who has made a request under the forgoing provisions of this section that the Data Controller in question has failed to comply with the request in contravention of those provisions, the court may order him/her to comply with the request.

10) In this section:
'prescribed' means prescribed by the Secretary of State by regulations;
The 'prescribed maximum' means such amount as may be prescribed;
'the prescribed period' means forty days or such other period as may be prescribed;
'the relevant day', in relation to a request under this section, means the day on which the Data Controller receives the request or, if later, the first day on which the Data Controller has both the required fee and the information referred to in subsection (3).

11) Different amounts or periods may be prescribed under this section in relation to different cases.

Section 8

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

2) The obligation imposed by section 7(1(c)(i) must be completed with by supplying the data subject with a copy of the information in permanent form unless:
   a) the supply of such a copy is not possible or would involve disproportionate effort, or
   b) the data subject agrees otherwise.

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

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

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

5) Section 7 (1)(4) is not to be regarded as requiring the provision of information as to the logic involved in decision-taking if, and to the extent that, the information constitutes a trade secret.

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

7) For the purposes of section 7(4) and (5) another individual can be identified from the information being disclosed if he/she can be identified from that information, or from that and any other information which, in the reasonable belief of the Data Controller, is likely to be in, the possession of the data subject making the request.
NOTE: These extracts are for guidance only. To ensure compliance

with the legislation, the relevant Data Protection legislation should be referred to in its entirety.

15. APPENDIX C – NATIONAL STANDARD FOR THE RELEASE OF DATA TO THIRD PARTIES.

15.1 INTRODUCTION:

Arguably CCTV is one of the most powerful tools to be developed during recent years to assist with efforts to combat crime and disorder whilst enhancing community safety. Equally, it may be regarded by some as the most potent infringement of people's liberty. If users, owners and managers of such systems are to command the respect of the general public, the systems must not only be used with the utmost probity at all times, they must be used in a manner which stands up to scrutiny and is accountable to the very people they are aiming to protect.

The Standards Committee of the CCTV User Group is committed to the belief that everyone has the right to respect for his or her private and family life and their home. Although the use of CCTV cameras has become widely accepted in the UK as an effective security tool, those people who do express concern tend to do so over the handling of the information (data) which the System gathers.

After considerable research and consultation, the following guidance has been adopted as a nationally recommended standard by the Standards Committee of the CCTV User Group and the Local Government Information Unit in consultation with CMG Consultancy.

15.2 GENERAL POLICY:

It is strongly recommended that local procedures should be put in place to ensure a standard approach to all requests for the release of data. It is recommended that every request is channelled through the Data Controller([1]) Notes([1]) The Data Controller is the person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal data are, or are to be, processed. (In most cases the Data Controller is likely to the scheme owner or manager).

15.3 PRIMARY REQUEST TO VIEW DATA:

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 reasons.

a) Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996, etc.)
b) Providing evidence in civil proceedings or tribunals.
c) The prevention of crime.
d) The investigation and detection of crime (may include identification of offenders).
e) Identification of witnesses.

1 Third parties, which should be required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:

a) Police ([1])
b) Statutory authorities with powers to prosecute, (e.g. Customs and Excise; Trading Standards, etc).
c) Solicitors ([2])
d) Plaintiffs in civil proceedings ([3])
e) Accused persons or defendants in criminal proceedings ([3])
f) Other agencies, (which should be specified in the Code of Practice) according to purpose and legal status ([4]).

2 Upon receipt from a third party of a bona fide request for the release of data, the scheme owner (or representative) should:

a) Not unduly obstruct a third party investigation to verify the existence of relevant data.
b) Ensure the retention of data which may be relevant to a request, but which may be pending application for, or the issue of, a court order or subpoena, (it may be appropriate to impose a time limit on such retention which should be notified at the time of the request). **NB** 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).
c) In circumstances outlined at note ([3]) below, (requests by plaintiffs, accused persons or defendants) the owner, (or nominated representative) should:
d) Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.
e) Treat all such enquiries with strict confidentiality.

Notes:

([1]) The release of data to the police may not be restricted to the civil police but could include, (for example) British Transport Police, Ministry of Defence Police, Military Police, etc. (It may be appropriate to put in place special arrangements in response to local requirements).

([2]) Aside from criminal investigations, data may be of evidential value in respect of civil proceedings or tribunals. In such cases a solicitor, or authorised representative of the tribunal, should be required to give relevant information in writing prior to a search being granted. In the event of a search resulting in a requirement being made for the release of data, such release will only be facilitated on the instructions of a court order or subpoena. It may be considered appropriate to make a charge for this service. In all circumstances data will only be released for lawful and proper purposes).

([3]) There may be occasions when an enquiry by a plaintiff, an accused person, a defendant or a defence solicitor falls outside the terms of disclosure or subject access legislation. An example could be the investigation of an alibi. Such an enquiry may not form part of a prosecution investigation. Defence enquiries could also arise in a case where there appeared to be no recorded evidence in a prosecution investigation. The scheme owner should decide which (if any) "other agencies" might be permitted access to data. Having identified those "other agencies", such access to data will only be permitted in compliance with this Standard. A Data Controller can refuse an individual request to view if insufficient or inaccurate information is provided. A search request should specify reasonable accuracy (could be specified in ½ hour).

15.4 SECONDARY REQUEST TO VIEW DATA:

1 A 'secondary' request for access to data may be defined as any request being made which does not fall into the category of a primary request. Before complying with a secondary request, the scheme owners should ensure that:

a) The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. Data Protection, section 163 Criminal Justice and Public Order Act 1994, etc.);

b) Any legislative requirements have been complied with, (e.g. the requirements of the Data Protection Act);

c) Due regard has been taken of any known case law (current or past) which may be relevant, (e.g. R v Brentwood BC ex p. Peck) and

d) The request would pass a test of 'disclosure in the public interest'([1])

2 If, in compliance with the secondary request to view data, a decision is taken to release material to a third party, the following safeguards should be put in place before surrendering the material;

a) 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 ([2]).

b) 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.

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

Notes

(1) Disclosure in the public interest could include the disclosure of personal data that:
   1 provides specific information which would be of value or of interest to the public well being
   2 identifies a public health or safety issue
   3 leads to the prevention of crime

(2) The disclosure of personal data which is the subject of a 'live' criminal investigation would always come under the terms of a primary request, (see **Paragraph 15.3** above).

15.5 INDIVIDUAL SUBJECT ACCESS UNDER DATA PROTECTION LEGISLATION:

1 Under the terms of Data Protection legislation, individual access to personal data, of which that individual is the data subject, must be permitted providing:

a) The request is made in writing;
b) A specified fee is paid for each individual search;
c) The Data Controller is supplied with sufficient information to satisfy him or her self as to the identity of the person making the request;
d) 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).
e) The person making the request is only shown information relevant to that particular search and which contains personal data of her or him self only, unless all other individuals who may be identified from the same information have consented to the disclosure.

2 In the event of the scheme owner complying with a request to supply a copy of the data to the subject, only data pertaining to the individual should be copied, (all other personal data which may facilitate the identification of any other person should be concealed or erased). Under these circumstances an additional fee may be payable.

3 The owner is entitled to refuse an individual request to view data under these provisions if insufficient or inaccurate information is provided. (However every effort should be made to comply with subject access procedures and each request should be treated on its own merit).

4 The code of practice should list procedures for the release of personal data. Before data is viewed by a third party, the Data Controller must be satisfied that data is:

a) Not currently and, as far as can be reasonably ascertained, not likely to become, part of a 'live' criminal investigation;
b) Not currently and, as far as can be reasonably ascertained, not likely to become, relevant to civil proceedings;
c) Not the subject of a complaint or dispute which has not been actioned;
d) The original data and that the audit trail has been maintained;
e) Not removed or copied without proper authority;
f) For individual disclosure only (i.e. to be disclosed to a named subject).

15.6 PROCESS OF DISCLOSURE:

1 Verify the accuracy of the request;

2 Replay the data to the requestee only, (or responsible person acting on behalf of the person making the request);

3 The viewing should take place in a separate room and not in the control or monitoring area. Only data which is specific to the search request should be shown;

4 It must not be possible to identify any other individual from the information being shown, (any such information should be blanked out, either by means of electronic screening or manual editing on the monitor screen[1]);

5 If a copy of the material is requested and there are no on-site means of editing out other personal data, then the material should be sent to an editing house for processing prior to being sent to the requestee.

Note

(1) The scheme owner is likely to breach Data Protection legislation if a person making a subject access request is able to identify any other individual from the information being disclosed. However a television image is two dimensional and the majority of CCTV schemes do not have immediate access to the necessary technology to blank out or remove 'other data'. It is recommended that the advice of the Data

Protection Registrar's office is sought in respect of any method which it is proposed should be adopted.

15.7 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:

1 In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' should be followed. If the material is to be released the following procedures should be adopted:

a) 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 of its use.

b) The release form should state that the receiver must process the data in a manner prescribed by the Data Controller, e.g. specify identities/data that must not be revealed.

c) It may also require that proof of editing must be passed back to the Data Controller, either for approval or final consent, prior to its intended use by the media (protecting the position of the Data Controller who would be responsible for any infringement of Data Protection legislation and the System's Code of Practice).

d) The release form should be considered a contract and signed by both parties(1).

Notes

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

15.8 PRINCIPLES:

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

1 Recorded material should be processed lawfully and fairly and used only for the purposes defined in the Code of Practice for the CCTV scheme;

2 Access to recorded material should only take place in accordance with this Standard and the Code of Practice;

3 The release or disclosure of data for commercial or entertainment purposes should be specifically prohibited.