DATA PROTECTION MODEL CODE OF PRACTICE IN RESPECT OF HUMBERSIDE POLICE CLOSED CIRCUIT TELEVISION (CCTV) SYSTEMS

1. PURPOSE

1.1 This Code of Practice provides a framework for the management and operation of existing or planned Humberside Police CCTV Systems to meet the requirements of the legislation and regulations governing their use. It also sets out the minimum standards required for the operation of such systems.

2. OBJECTIVES

2.1 In order to comply with the Data Protection Act, CCTV must only be used for the following defined purposes

- To assist with the prevention and detection crime.
- To identify offenders.
- To be of use as evidence within the Criminal Justice System.
- To reduce the fear of crime.
- To promote safer communities.
- To improve road safety and traffic flow.
- To assist in the development of traffic management schemes.
- To improve officer and staff safety.
- To prevent anti-social behaviour
- To prevent and detect damage to property

3. PRINCIPLES

3.1 CCTV systems operated under this Code of Practice will be used to monitor and record images from public places in accordance with the objectives shown in paragraph 3.1 above. Images will be transmitted to a secure recording/monitoring environment that meets the requirements of the legislation in terms of both staffing and technical specification.

3.2 When required, the systems will provide the means by which evidence can be adduced by any person or body having lawful reason for accessing the recorded images and such evidence may subsequently be made available for court proceedings.

3.3 Specialist and covert surveillance by Police and other agencies is not covered by these codes of practice. In cases where specific monitoring is required, which falls outside of this code, appropriate authority must be obtained in order to comply with legislation. Advice will be included within the system's Operating Procedure Manual on how to obtain the necessary authority.

3.4 This code will observe all aspects of the Human Rights Act 1998 particularly Articles 6 (Right to a Fair Trial) and 8 (Right to Respect for Private and Family Life), and will incorporate those safeguards necessary to protect the rights of privacy, except where the law permits specific surveillance activities.

3.5 If such information is to be exchanged, information-sharing protocols will be established prior to such exchange-taking place.

3.6 This Code should apply to the development of future systems and to the expansion of existing ones.

3.7 <u>This document shall be reviewed annually by the Crime Reduction Policy Unit to ensure that it continues to meet current requirements.</u>

3.8 Any changes to working practices as set out in the Operating Procedure Manual should be agreed and implemented by the CCTV Working Group.

4. DEFINITIONS

4.1 **Identify** - shall mean that picture quality and detail should be sufficient to enable the identity of a subject to be established beyond reasonable doubt. This will require an image size of not less than 120%R as defined in The Police Scientific Development Branch C.C.T.V. OPERATIONAL REQUIREMENTS MANUAL publication number 17/94.

4.2 **Images** shall refer to and include all images, audio, or any other data, whether live or recorded, on any media, in any format.

5. DATA PROTECTION ACT 1998

5.1 The Information Commissioner has issued a Code of Practice under Section 51 (3)(b) of the Data Protection Act 1998. The full code is available on the Data Protection web site **(www.dataprotection.gov.uk).**

5.2 All parties processing or monitoring images will be required to notify the Information Commissioner's Office of their involvement. Failure to do so may result in an order being issued by the Commissioner to cease operating and subsequent prosecution. Prosecutions could be pursued against the Data Controller (whether personal or corporate) or against any officer who fails to carry out their duties under the Act.

5.3 This code follows the sections 1 & 2 of The Data Protection Act 1998 in defining the following:-

- Data Controller
- Personal Data
- Sensitive Personal Data
- Processing

6. INTRODUCTION TO CODE.

6.1 The Code applies to all CCTV systems and similar surveillance equipment used for monitoring and recording images from those **areas to which the public have largely free and unrestricted access.**

6.2 This code does NOT apply in the instances where "appropriate authority" has been obtained under the Regulation of Investigatory Powers Act 2000.

6.3 This code of practice will be revised when necessary to take into account the following-

- The interpretation of the provisions of the Data Protection legislation.
- The changes in technology involved in recording images.
- The use of such technology.
- Other legislation introduced to cover the use of CCTV.

6.4 Full consultation will take place when such changes are necessary.

The Chief Constable is the Data Controller for which the responsibility will be devolved accordingly.

6.5 For every system, Humberside Police will undertake the following:

- Identify the person(s) or organisation(s) legally responsible for the management and operation of the various systems (Divisional /Branch Managers and Liaison Officers) in accordance with the First Principle of the Act.
- Assess the appropriateness and reasons for using the CCTV or similar surveillance equipment. (First Principle) (Home Office Standard Security Survey of Police Stations, Buildings & Estates). Conducted by Divisional Crime Prevention Officers.
- Define the purpose and objectives of the systems (First and Second Principles)
- Notify the Information Commissioner in writing of the above information (Force Data Protection Officer)
- Ensure the systems and operations thereof comply with the Human Rights Act 1998
- Maintain appropriate records to support the running of the respective systems
- Define and maintain an Operating Procedure Manual for all parties involved.

6.6 Signs will be placed in the proximity of the system so that the public is aware they are entering a zone covered by surveillance equipment. The signs will be clearly visible to the public, be an appropriate size and contain the following information;

6.7 Where no pictogram is used:

- The identity of the person or organisation responsible for the system
- The phone number of the person or organisation
- The purpose of the system

For example;

Humberside Police Tel: 01482 326111 **This area is covered by CCTV used for Crime Reduction purposes"**

6.8 Where a pictogram is used:-

- The phone number of the person or organisation responsible for the system
- The identity of the person or organisation responsible for the system

For example;

"Image' **01482 326111** **Humberside Police**

6.9 In exceptional circumstances, signs may not be placed. In this case, the operators must have assessed (and documented) that they have:-

a. Identified specific activity
b. identified the need to use surveillance to obtain evidence of that criminal activity
c. That the use of the signs would prejudice success in gathering that evidence
d. Assessed how long the covert monitoring should continue to avoid unnecessary observation.
e. Obtained the requisite permission for such surveillance

7. POSITIONING OF CAMERAS

7.1 The location of cameras and the means by which images are captured must comply with the First Data Protection Principle.

7.2 Cameras will be situated where they only capture images relevant to the purpose for which the system has been established. (see section 2.1 above) For example, if a camera is located for the prevention and detection of crime, it should be capable of capturing facial images to identify suspects and/or offenders

7.3 Individual Camera siting will take place on the basis of an operational requirement setting out the purpose of each camera.

7.4 Cameras will be sited in such a way as to monitor only those areas to which the public has access. Where it is not possible physically to prevent cameras from viewing private areas, then other means such as electronic **"privacy zones"** should be used to electronically mask out these areas. Staff must be suitably trained and made aware of the privacy implications under the Data Protection and Human Rights Acts.

7.5 Images so obtained will be used only to achieve the objectives of the system and for no other purposes.

7.6 If the equipment has sound recording facilities, it will only be used to achieve the objectives of the system. It will not be used to record conversation between members of the public in public areas.

8. QUALITY OF IMAGES.

8.1 It is of the utmost importance that images recorded by the equipment are of sufficient quality to be effective for the purposes for which they are made (Third Principle). It is essential that cameras positioned for crime detection and/or prevention should be capable of good quality images able to identify suspects and offenders.

8.2 The System will have an appropriate maintenance regime so as to maintain this quality and cameras that fail to reach the appropriate level of quality will be changed or removed from the system. Suitable safeguards will exist to prevent cameras from being tampered with or vandalised. The method of dealing with repairs etc. will be documented.

8.3 High quality image recording media will be used at all times.

8.4 If the system is developed to include a method of facial recognition, then operators will have access to both the data base image and the camera image so that a human comparison can be made to verify an accurate match. Both these images will be clear enough for this human comparison to take place. Any such comparisons undertaken will be documented, whether or not a match was concluded

9. SECURITY OF SYSTEM.

9.1 Security of Images and the Monitoring centre is essential and must be maintained at all times to comply with the Data Protection Act 1998 (Seventh Principle)

9.2 Access to monitoring areas and other viewing areas will be restricted to designated/named members of staff and other authorised persons. Operators will sign on and off duty in the appropriate register. All visitors to the room must be accompanied at all times by a manager or designated person and the visit must comply with the guidelines set out in the Operating Procedures (See Appendix C).

9.3 Access to recorded images will be restricted to a manager or designated members of staff, who will decide whether to allow requests from third parties in accordance with the documented disclosure policies.

9.4 An Ethics Committee will be established by Humberside Police who will consider any requests for access which are not covered by this Code of Practice, receive complaints regarding the operation of respective CCTV systems and generally monitor compliance of the systems with this Code of Practice.

9.5 Viewing of images will take place in a restricted and private area. It is essential that no general access is permitted to other employees and staff unless performing duties in accordance with CCTV monitoring and management. The basis for this restriction is to protect the privacy rights of members of the public and to avoid compromising persons who view the monitors. (Seventh Principle).

9.6 All operators and employees with access to images will be aware of the procedures for image or data management and limitations of access to images and of the sanctions available for breaching such procedures.

9.7 All operators will be trained in their responsibilities under this Code of Practice. They will be aware of:-

a. Security Policy for monitoring rooms and image control
b. Disclosure policy (see Access and Disclosure below)
c. Rights of individuals in relation to personal data.

10. ACCESS TO AND DISCLOSURE OF IMAGES TO THIRD PARTIES.

10.1 Access to and disclosure of images (live and recorded) by CCTV and similar surveillance systems will be restricted and carefully controlled to ensure the rights of individuals are preserved. This will also ensure the chain of evidence remains intact, should the images be required for evidence.

10.2 Any processing of images must be carried out in accordance with the following Principles:-

- Employee and staff access to recorded images is restricted to those who need to know. (Seventh Principle)
- All access to images must be documented
- Access to images by third parties will only be allowed in limited and prescribed circumstances. i.e., if the purpose of the system is the prevention and detection of crime, then disclosure to third parties maybe limited to the following
    - Law enforcement agencies where the images recorded would assist in a specific criminal enquiry
    - Prosecution agencies (DSS, Customs & Excise etc.)
    - Legal representatives of defendants or complainants.
    - The media, where it is assessed by the Police, that the public's help is needed in order to assist in the identification of a victim, witness or perpetrator in relation to a criminal incident. (see operating procedures for process and guidance on victims wishes)
    - Individuals who have been recorded and have a right of access under the Data Protection Act 1998 (unless disclosure would prejudice a criminal enquiry or criminal proceedings)
    - Police forces where the sole purpose is to use images for the training of police officers, managers and operators.
- All requests for access to images or requests for copies will be fully documented (DPSA1A). If access or disclosure is denied, the reason(s) will be fully documented. Appropriate forms will be held at the Data Protection Section and Front Enquiry Desks for members of the public to apply for access.

10.3 When access or disclosure is allowed, then the following will be documented:

- The date and time at which access was allowed or the date on which disclosure was made.
- The identification of any third party that was allowed access or to whom disclosure was made.
- The reason for allowing access or disclosure. (not required from subject)
- The extent of information to which access was allowed or disclosed.

10.4 Recorded images will not be made available to the media or placed on the Internet (Second, Seventh and Eighth Principles). This does not preclude the use of traffic cameras

which are broadcast live on the Internet and which are not capable of identifying a living individual.

10.5 If it is intended that images are to be made more widely available, the decision will be made by the system manager and the Ethics Committee. The reason for that decision will be documented and will comply with the Police and Criminal Evidence Code of Practice if applicable.

10.6 If images are released to the media in the above circumstances the images of non-relevant individuals or other identifying data will be disguised or blurred. (First, Second and Seventh Principles)

10.7 If the system does not have the ability to carry out that type of editing, a suitable editing contractor will be employed. Where such an external company is hired, there will be a contractual relationship between the data controller and editing company to ensure the following

- The editing company had given appropriate guarantees regarding the security measures they take in relation to the images.
- The manager has checked to see those guarantees are in place.
- The written contract makes it clear that the editing company can only use the images in accordance with the instructions of the manager or designated member of staff.
- The written contract makes the security guarantees provided by the editing company explicit. (Seventh Principle)

The system manager will ensure that contractors are aware of the above and ensure compliance. (The Technical Support Unit (TSU) is in a position to conduct editing)

10.8 If the media organisation undertakes the editing, then para 10.6 will apply.

11. ACCESS BY DATA SUBJECTS.

11.1 The right to images of Individuals by that individual is provided for in section 7 of the Data Protection Act 1998 and should be afforded wherever possible.

11.2 All relevant staff must be able to recognise a request for access to recorded images by data subjects**.** (Sixth and seventh Principles).

11.3 People requesting data subject access will be provided with a standard 'subject access request' form (DPSA1A) that;-

- Indicates the information required to locate the images requested.
- Indicates the information required to identify the person making the request.
- Indicates the fee that will be charged for carrying out the search for the images requested. (Currently £10 and set by statute).
- Ask whether the individual only wishes to view the images or whether a copy is required.
- Indicates that a response will be made promptly and no longer than 40 days from the day the request was received (which will be endorsed on the form).

11.4 Individuals will be provided with a leaflet (DPSA1A-CCTV) describing the types of images recorded and retained the purpose for which those images are recorded and retained and information about the disclosure policy in relation to those images. (Sixth Data Protection Principle)

11.5 All subject access requests will be dealt with by the Force Data Protection Officer (DPO). Where possible, the DPO or designated member of staff will locate the images requested.

11.6 The DPO or designated member of staff will determine whether disclosure to the individual will entail disclosing images of third parties. Similarly, he/she will decide if the images are held under a duty of confidence. It is likely that a member of the public walking in a public area will reasonably have less expectation that their images are held under a duty of confidence than those recorded for example in a police waiting room.

11.7 If third party images are not to be disclosed, they will be disguised or blurred out.

11.8 If the DPO OIC (officer in the case) or a designated member of staff decides that a subject request form should not be complied with, he/she will document fully the following:-

- The identity of the individual making the request.
- The date of the request
- The reason(s) for refusing to supply the images requested.
- The name and signature of the DPO or Decision-Maker.

11.9 All staff will be made aware of the individuals' rights under this section of the Code of Practice. (Sixth Principle).

12. OTHER INDIVIDUALS' RIGHTS.

12.1 The disclosure or viewing of images may compromise third parties, depending on the content of the images. The Data Protection Act 1998 makes provision for other individuals' rights to be taken into account.

12.2 Section 10 of the Act provides the individual the right to prevent processing which is likely to cause damage or distress. Operators and managers must have a clear understanding of these rights, to avoid leaving the data controller open to civil litigation.

12.3 All staff must be able to recognise a subject access request from an individual in order to deal with the request as per the below Force Policy following the requirements of the Data Protection Act:

Where an individual requests access to a CCTV recording of him/herself, this will be dealt with as per Section 7 Data Protection Act 1998.

As with any other request for access to 'personal data' the applicant should be provided with a form DPSA1A (subject access request form available from any enquiry office).

For CCTV applications an additional leaflet DPSA1A – CCTV (Appendix F of OPM) should be supplied for guidance to the applicant on completing the application.
The completed application form and relevant videotape should be forwarded to the Data Protection Officer without delay. The videotape tracking sheet (Appendix H) should be endorsed accordingly and the videotape transferred in accordance with Practice Direction GPMS (Government Protection Marking Scheme) restricted rules.

The Force Data Protection Officer will liase with the applicant and make the necessary arrangements through the Technical Support Unit, to meet the requirements of the request under Section 7 (1) C and 8 (2) of the Act.

A request must be satisfied within 40 days of receiving a completed application.

13. COMPLIANCE WITH CODE OF PRACTICE

13.1 The operators of the Humberside Police Systems will comply with this Code of Practice. There will be an Ethics Committee established to ensure

- compliance with the codes
- public support for the system is maintained
- continued ethical use of the system

13.2 The contact point indicated on the signs within the area covered by CCTV will be available to members of the public during office hours. The following information will be made available at the specified location:-

- Copies of the leaflet setting out subject access rights.
- A copy of the code of practice.
- Subject access request form.
- Details of the complaint procedure should they have concerns about the use of the system.
- Details of the complaint procedure to be followed where they may have concerns about non-compliance with the provision of this code.

13.3 The complaint procedure will be fully and clearly documented and a record of all complaints received will be maintained. These records will be taken into account when assessing the effectiveness of the overall scheme

13.4 The Ethics Committee will provide a report reviewing complaints for the data controller(s) in order that compliance with legal obligations and provisions with this code of practice can be monitored.

13.5 An annual report will be compiled (Divisional CPO's) which evaluates the effectiveness of the respective systems and sets out recommendations for any improvements or changes so as to ensure the systems comply with the stated purposes, objectives and aims. This report will be made available to all the interested partners.

13.6 From the above document the systems managers will compile a public report setting out the details of their respective systems and outlining the effectiveness, giving examples of successes in order to maintain public support. This will not include technical specifications of systems.

14. TECHNICAL STANDARDS.

14.1 The System Managers, together with the Communications Branch Manager and Divisional Crime Prevention Officers, will, notwithstanding the requirements of the Data Protection Act 1998, carry out annual assessments so as to meet a minimum technical requirements. This should be done in conjunction with an operational requirement specification for each camera and the Home Office recommendations for CCTV design.(PSDB Publications)

14.2 Where technical improvements can be made to the operational effectiveness of the system, recommendations will be documented and submitted to the Communications Branch for consideration and discussion under the Best Value scheme.

14.3 If it is necessary to make environmental changes affecting the performance of the system, the System Manager will facilitate the changes to be made to improve or maintain its operational effectiveness e.g. trees obscuring camera views may need pruning. This process will be fully documented.

15. MONITORING AT LOCATIONS OTHER THAN THE PRINCIPAL CONTROL ROOM.

15.1 This Code of Practice will apply, in full, wherever monitoring or processing of images from the system takes place.

16. ACCESS TO EQUIPMENT.

16.1 Access to equipment will be restricted to only those contractors and staff who have direct responsibility for that equipment. Under no circumstances will unqualified staff attempt technical access.

16.2 When contractors carry out work on CCTV equipment, the duty operator or manager will be made aware of the work being undertaken. This is to ensure that safety regulations are complied with in the CCTV monitoring area. (see section on Health & Safety below)

16.3 Except in emergency situations, as far as is possible, such work will be pre planned and carried out so as not to interfere with the normal working of the system.

17. OPERATING PROCEDURE MANUAL

17.1 The system will have in place an operating and best practice manual setting out the day to day guidelines of operating the system in accordance with the Code of Practice. This will contain local instructions and policy and ensure that manufacturers operating instructions are complied with.

17.2 This manual will not be a public document.

17.3 Any major changes in this manual will be discussed and agreed with all interested partners (CCTV working group). Minor changes will be agreed locally by the system manager.

18. TRAINING.

18.1 All staff employed to operate the system will be screened in accordance with the partners policy,

18.2 All staff will be trained to a suitable level in all technical, operational and ethical aspects of the system. This will assist in the implementation of these codes of practice and ensure that evidence gathered will be of a suitable quality.

19. HEALTH AND SAFETY.

19.1 All CCTV monitoring centres are places of work for the purposes of the Health and Safety at Work regulations and are subject to the normal risk assessments, which will be carried out in accordance with the Humberside Police normal practice.

19.2 At no time will unqualified staff undertake maintenance or interfere with equipment other than in accordance with the guidelines issued by manufacturers for normal operating procedures.

19.3 The system manager will maintain records of all work carried out on the system.

19.4 Up to date Health and Safety signs will be displayed within CCTV monitoring centres and suitable first aid facilities made available.

19.5 Working practices will comply with the employer current policy and government or Health and Safety regulations. Hours of work will be recorded in the normal manner and the system manager will be responsible for maintaining agreed staffing levels.

19.6 At no time will staff be expected to carry out duties that would bring them into conflict with Health and Safety regulations.

20. SECURITY OF DATA.

20.1 The security of all images or data on the system is of the utmost importance.

20.2 To this end only those persons who have a legitimate need to view the images in connection with their role or job will be allowed to view any images.

20.3 Such an authorised person will be required to identify themselves to the system by means of a log on name and password. Such passwords will be reviewed on a regular basis. The system manager will control access.

20.4 Images will not be retained for longer than is necessary to comply with the objectives of the system. Generally only evidential images will be retained (Fifth Principle)

20.5 Images retained for these purposes will be securely stored so as to ensure their integrity is maintained. This will also ensure that the evidential value is maintained to protect the rights of members of public who may have been recorded.

20.6 Access to these images will be carefully controlled and restricted to those persons who have access under the Data Protection Act 1998. (Seventh Principle).

20.7 Images will only be released to those persons who have a legal right to view them.

20.8 Images removed for evidence or access will be documented fully to include at least the following information:-

a. The date on which they were taken out of use and by whom
b. The reason they were removed
c. Any crime or other unique reference number for cross reference purposes
d. Where the tape is stored or to whom it was handed
e. The details and signature of the person taking possession.

20.9 The system manager may deny access to the system by any user without giving reason.

20.10 Every activity carried out on the system will be recorded and available for inspection by the system manager, the Ethics Committee or a Court of Law.

20.11 All equipment will be housed in secure buildings accessible only via the system manager.

20.12 The system will be designed to be totally self contained and will not be accessible by any physical or electronic means except to authorised persons.

20.13 Details of other means of protecting the all data will not be made public and will only be made available to a court of law if required.

APPENDIX A

Data Protection Act 1998 - Principles

The Standards;

Anyone processing personal data must comply with the eight enforceable principles of good practice. They say that data must be: -

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than necessary;
- processed in accordance with the data subjects rights;
- secure;
- Not transferred to other countries without adequate protection.

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual, although in some limited circumstances exemptions will apply. With processing, the definition is far wider than in the 1984 Act. For example, it incorporates the concepts of 'obtaining', holding' and 'disclosing'

1. Definitions

There are several definitions in Sections 1 and 2 of the l998 Act which users of CCTV systems or similar surveillance equipment must consider in order to determine whether they need to comply with the requirements of the l998 Act, and if so, to what extent.

a) Data Controller
"A 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, or are to be, processed".

For example: Humberside Police installs CCTV in Police buildings and estates with a view to: -

- Preventing and detecting crime.
- Apprehending and prosecuting offenders.
- Protecting public safety.

"The Data Controller solely responsible for those Humberside Police Systems is the Chief Constable".

Where Humberside Police, a local authority and local retailers decide to install a CCTV scheme in a town centre or shopping centre, for the purposes of:

- Prevention or detection crime.
- Apprehending or prosecuting offenders.
- Protecting public safety.

All will be data controllers for the purposes of the scheme. It is the data controllers who should set out the purposes of the scheme (as outlined above) and who should set out the policies on the use of the images (as outlined in the Standards section of this Code of Practice).

The data controller(s) may devolve day-to-day running of the scheme to a manager, but that manager is not the data controller - he or she can only manage the scheme according to the instructions of the data controller(s), and according to the policies set out by the data controller(s).

If the manager of the scheme is an employee of one or more of the data controllers, then the manager will not have any personal data protection responsibilities as a data controller. However, the manager should be aware that if he or she acts outside the instructions of the data controller(s) in relation to obtaining or disclosing the images, they may commit a criminal offence contrary to Section 55 of the l998 Act, as well as breach their contract of employment.

If the manager is a third party such as a security company employed by the data controller to run the scheme, then the manager may be deemed a data processor. This is "any person (other than an employee of the data controller) who processes the personal data on behalf of the data controller". If the data controller(s) are considering using a data processor, they will need to consider their compliance with the Seventh Principle in terms of this relationship.

b) Personal Data

"Data which relate to a living individual who can be identified:

a) from those data, or
b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller".

The provisions of the l998 Act are based on the requirements of a European Directive European Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data which, at Article 2, defines, personal data as follows:

"Personal data" shall mean any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

The definition of personal data is not therefore limited to circumstances where a data controller can attribute a name to a particular image. If images of distinguishable individuals' features are processed and an individual can be identified from these images, they will amount to personal data.

c) Sensitive Personal Data
Section 2 of the l998 Act separates out distinct categories of personal data, which are deemed sensitive. The most significant of these categories for the purposes of this code of practice are information about: Section 2 of Act sets out the full list of categories of sensitive personal data. This part of the Code only refers to some of the categories, which may have particular relevance for users of CCTV. For a full list, please see the relevant section of the Act.

- the commission or alleged commission of any offences
- any proceedings for any offence committed, or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

This latter bullet point will be particularly significant for those CCTV schemes which are established by retailers in conjunction with the local police force, which use other information to identify known and convicted shoplifters from images, with a view to reducing the amount of organised shoplifting in a retail centre.

It is essential that data controllers determine whether they are processing sensitive personal data because it has particular implications for their compliance with the First Principle.

d) Processing
Section l of the l998 Act sets out the type of operations that can constitute 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, including:
a) organisation, adaptation 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."

The definition is wide enough to cover the simple recording and holding of images for a limited period of time, even if no further reference is made to those images. It is also wide enough to cover real-time transmission of the images. Thus if the images of individuals passing in front of a camera are shown in real time on a monitor, this constitutes "transmission, dissemination or otherwise making available. Thus even the least sophisticated capturing and use of images falls within the definition of processing in the l998 Act.

APPENDIX B

REGULATION OF INVESTIGATORY POWERS ACT 2000.

Surveillance is **Directed Surveillance** where it is covert, but not intrusive, and is undertaken:

a) for the purposes of a specific investigation or operation; and

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 an 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.

Surveillance is **Intrusive Surveillance** if, and only if, it is covert surveillance that-

a) (a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

b) (b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

Appendix C

Public Access

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

Authorised Visits

Visits by inspectors of CCTV Systems 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 of CCTV systems or auditors will visit at any one time. Inspectors of CCTV systems 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.

Declaration of Confidentiality

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

Note: It is recommended that each page of the Visitor Book include a declaration of confidentiality as a constant reminder of their obligations. Recommended wording be as follows: -

'In signing this visitors book all visitors to the Name of system CCTV monitoring room acknowledge that the precise location of the CCTV monitoring room and personal details of those operating the system, is, and should remain confidential. They further agree not to divulge any information obtained, overheard or overseen during their visit.'

It is also best practice to display a notice at the entrance to the room that they are entering a restricted area, and entry is dependent upon acceptance of the need for confidentiality. A typical notice is included overleaf.

WARNING

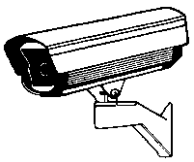
RESTRICTED ACCESS AREA

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'.

Final Draft

HUMBERSIDE POLICE



Code of Practice

In respect of the operation of

Humberside Police

Closed Circuit Television Systems