Bolton Council

Together in Partnership

CCTV

Code of Practice

November 2008

CONTENTS

1. Introduction and Objectives

1.1. Introduction

A Closed Circuit Television (CCTV) System is operational within Bolton. This System, known as the Bolton CCTV System, comprises a number of cameras installed at strategic locations. The cameras are fully operational and either fixed or with pan, tilt and zoom facilities. The System is operated from a Control Centre within the town.

1.2. Definitions

- For the purposes of this document, the **'owner'** of the system is
- For the purposes of the Data Protection Act the **'data controller'** is Bolton Bolton Council
- For the purposes of this document, the **'System Manager'**: means NCP's CCTV Services Manager.
- Details of key personnel, their responsibilities and contact points are shown at appendix A.1 to this Code.

1.3. Partnership statement in respect of The Human Rights Act 1998

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

Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for local authorities to provide closed circuit television coverage of any land within their area for the purposes of crime prevention or victim welfare. The Local Authorities and Police also consider it a necessary initiative towards their duty under the Crime and Disorder Act 1998.

The Bolton CCTV System shall be operated with respect for all individuals, recognizing the right to be free from inhuman or degrading treatment and avoiding discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status. Further the System shall be operated in such a way as to avoid infringement of individual privacy.

The Council recognises that it is their responsibility to ensure that the scheme should always comply with all relevant legislation, to ensure its legality and legitimacy. The scheme will only be used as a proportional response to identified problems and be used only in so far as it is necessary in a democratic society, in the interests of national security, public safety, the economic well being of the area, for the prevention and detection of crime or disorder, for the protection of health and morals, or for the protection of the rights and freedoms of others.

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

1.4. Objectives of the System

The objectives of the Bolton CCTV System as determined by the Data Controller and which form the lawful basis for the processing of data are:

- To provide a tool by which the permitted or authorised 'users' may better and more efficiently undertake their departmental, business unit or contractual responsibilities for the Council.
- Assist in the detection, prevention and deterrence of crime and disorder in the area this will include:
    - Countering terrorism
    - Helping to identify, apprehend and prosecute offenders,
    - Provide the police, other agencies and the Council with evidence to take criminal and civil action in the courts
- To help reduce the fear of crime and provide reassurance to the public
- To increase public safety for those people who live, work, trade and visit Bolton
- To assist in the overall management of the public space
- To help deter and detect acts of anti-social behaviour
- To enhance community safety, assist in developing the economic well being of the Bolton area and encourage greater use of the Town Centre
- To assist in the enforcement and regulatory functions within the Bolton area
- To assist in Traffic Management
- To assist in monitoring any Emergency Planning Operations
- To assist members of the public, businesses or professional individuals with their requests for the appropriate or permitted information pertaining to incidents that may occur within the Bolton area

Within this broad outline, the Data Controller may draw up specific key objectives (which will be reviewed annually) based on local concerns.

1.5. Operational Guidance

This Code of Practice (hereafter referred to as 'the Code') is supplemented by separate 'Operational Instructions' which offers instructions on all aspects of the day to day operation of the system. To ensure the purpose and principles (see Section 2) of the CCTV system are realised, the Operational Instructions are based and expand upon the contents of this Code of Practice.

2. Statement of Purpose and Principles

2.1. Purpose

The purpose of this document is to state how the owners and the managers, intend to use the Bolton CCTV System, (hereafter referred to as 'The System') to meet the objectives and principles outlined in Section 1.

2.2. General Principles of Operation

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

The operation of the System will also recognise the need for formal authorisation of surveillance as required by the Regulation of Investigatory Powers Act 2000, in particular Part 2 of the Act, and the police force policy.

The System will be operated in accordance with the Data Protection Act 1998 at all times.

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

The System will be operated with due regard to a general right to respect for his or her private and family life and their home.

The public interest in the operation of the System will be safeguarded by ensuring the security and integrity of operational procedures.

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

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

2.3. Copyright

Copyright and ownership of all material recorded by virtue of The System will remain with the Data Controller.

2.4. Cameras and Area Coverage

This Code of Practice refers are to those areas within the responsibility of the operating partners.

Where mobile cameras are deployed, they will be remotely connected to the control centre and their operation will be similar to fixed camera installations.

All cameras within the System will be positioned within an area suitably signed to alert of their presence.

2.5. Monitoring and Recording Facilities

All cameras are connected to the System's control centre. All images captured by the System are recorded throughout every 24 hour period by the control centre designated for that purpose.

2.6. Human Resources

Unauthorised persons will not have access without an authorised member of staff being present.
The control room shall be staffed by specially selected and trained operators in accordance with the requirements of the Security Industry Act.
All operators shall receive training relevant to their role in the requirements of the Human Rights Act 1998, Data Protection Act 1998, Regulation of Investigatory Powers Act 2000 and the Codes of Practice and Operating Instructions. Further training will be provided as necessary.

2.7. Processing and Handling of Recorded Material

No recorded material will be released from the control center unless it is in accordance with this Code of Practice.

2.8. Operators Instructions

The control room has its own Operational Instructions, which comply with this Code of Practice.

2.9. Changes to the Code

Any major changes to the Code of Practice, will take place only after consultation with, and upon the agreement of the Partnership.

A minor change, (i.e. such as may be required for clarification and will not have such a significant impact) may be agreed between the System Managers and the Owners of the System.

Notes:

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

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

- Bolton Council will not utilise 'dummy' cameras. The greatest deterrent value of a CCTV System is its power to produce evidential material and, in doing so, to reassure those it is intended to protect.

3. Privacy & Data Protection

3.1. Public Concern

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.

'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;

- organisation, adaptation or alteration of the information or data;
- retrieval, consultation or use of the information or data;
- disclosure of the information or data by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data.

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

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

Cameras will not be used to look into private residential property, unless pursuing a suspect and this is considered to be in the interests of the private residents. Operators will be specifically trained in privacy issues.

3.2. Data Protection Legislation

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

The 'data controller' for The System' is Bolton Council and day to day responsibility for the data will be devolved to the NCP CCTV System Manager.

All data will be processed in accordance with the principles of the Data Protection Act, 1998 which are in summarised form:

- All personal data will be processed fairly and lawfully.
- Personal data will be obtained only for the purposes specified.
- Personal data held will be adequate, relevant and not excessive in relation to the purpose for which the data is processed.
- Steps will be taken to ensure that personal data is accurate and where necessary, kept up to date.
- Personal data will be held for no longer than is necessary.
- Individuals will be allowed access to personal data, in accordance with individual's rights.

- Procedures will be implemented to ensure security measures to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of, information.
- Information shall not be transferred outside the European Economic Area unless the rights of individuals are protected.

3.3. Request for information (subject access)

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

The principles of the Data Protection Act 1998 shall be followed in respect of every request. Individuals whose image is captured on CCTV are entitled to make an access request.

If the request cannot be complied with without identifying another individual, permission from that individual must be obtained, unless it is reasonable in all the circumstances to comply with the request without the consent of that individual.

Any person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located.

3.4. Exemptions to the Provision of Information

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

Personal data processed for any of the following purposes –

- the prevention or detection of crime
- the apprehension or prosecution of offenders

are exempt from the subject access provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the matters referred to above.

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

3.5. Criminal Procedures and Investigations Act, 1996

The Criminal Procedures and Investigations Act, 1996 came into effect in April, 1997 and introduced a statutory framework for the disclosure to defendants of material which the prosecution would not intend to use in the presentation of its own case, (known as unused material). An explanatory summary of the provisions of the Act is contained within the Operational Instructions, 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).

4. Accountability and Public Information

4.1. The Public

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 with legitimate reasons 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.

Cameras will not be used to look into private residential property, unless pursuing a suspect and this is considered to be in the interests of the public.

A member of the public wishing to register a complaint with regard to any aspect of The System may do so by contacting the NCP CCTV Services Manager's office. All complaints shall be dealt with in accordance with the Bolton Council complaints procedure (as appropriate), a copy of which may be obtained from Bolton Council offices. Any performance issues identified will be considered under the relevant organisations disciplinary procedures to which all employees, including CCTV personnel are subject.

- Telephone: 01204 336902
- Email: Boltoncctvoperatives@NCP.co.uk
- Write to: NCP Bolton, Bolton Town Hall, Victoria Square, Bolton, BL1 1RU.

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

4.2. System Manager

The NCP CCTV System Manager will have day-to-day responsibility for the System as a whole. The CCTV System will be subject to the usual Local Government audit arrangements.

4.3 Public Information

Code of Practice
A copy of this Code of Practice shall be published on the Bolton Council web site, and a copy will be made available to anyone on request.

Signs
Signs have been placed in the locality of the cameras and at main entrance points to the relevant areas. The signs will indicate:

- The presence of CCTV monitoring;
- The purpose for the scheme
- The 'ownership' of the System;
- Contact telephone number for the System.

5. Assessment of the System and Code of Practice

5.1. Monitoring

The NCP CCTV System Manager will accept day-to-day responsibility for the monitoring and operation of the System and the implementation of this Code of Practice.

The NCP CCTV System Manager shall also be responsible for maintaining full management information as to the incidents dealt with by the monitoring room, for use in the management of the System and in future evaluations

5.2. Audit

There will be regular audits of the operation of the System and the compliance with this Code of Practice. Audits, which may be in the form of irregular spot checks, will include examination of the monitoring room records, media histories and the content of recorded material.

6. Human Resources

6.1. Staffing of the Monitoring Room

The CCTV Monitoring Room will be staffed in accordance with the Operational Instructions. Equipment associated with The System will only be operated by authorised personnel who will have been properly trained in its use and all monitoring room procedures.
Every person involved in the management and operation of the system will be personally issued with a copy of both the Code of Practice the Operational Instructions, and will be required to sign a confirmation that they fully understand the obligations adherence to these documents places upon them and that any breach will be considered as a disciplinary offence. They will be fully conversant with the contents of both documents, which may be updated from time to time, and which he / she will be expected to comply with as far as is reasonably practicable at all times.
Arrangements have been made for police officers to be present in the monitoring room at certain times, subject to locally agreed protocols. Any such person must also be conversant with this Code of Practice and associated Operational Instructions, if operating the CCTV system.

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

6.2. Discipline

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

6.3. Declaration of Confidentiality

Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with the system to which they refer, will be required to sign a declaration of confidentiality.

7. Control and Operation of Cameras

7.1. Guiding Principles

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

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

Cameras will not be used to look into private residential property, unless pursuing a suspect and this is considered to be in the interests of the public. (See Section 4).

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

7.2. Primary Control

Only those trained and authorised members of staff with responsibility for using the CCTV equipment will have access to the operating controls, those operators have primacy of control at all times. Authorised Police Officers are also permitted to use the equipment. Police officers (Guests) who are not authorised personnel may work within the control room but must not operate the CCTV System.

7.3. Secondary Control

Secondary recording and reviewing facilities are provided at Bolton Central Police Station. No access to the movement of cameras is given at this facility.

7.4. Operation of The System by the Police

The Police may make a request to assume control of the system to which this Code of Practice applies. Only requests made on the written authority of a police officer of Superintendent rank or above will be considered. Any such request will only be accommodated on the personal written authority of the most senior representative of the Owners, or designated deputy of equal standing.

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

In very extreme circumstances a request may be made for the Police to take total control of the system in its entirety, including the staffing of the monitoring room and personal control of all associated equipment, to the exclusion of all representatives of the Owners.
Any such request must be made to The NCP CCTV System Manager in the first instance, who will consult personally with the most senior officer of The Owners (or designated deputy). A request for total exclusive control must be made in writing by a police officer of the rank of Assistant Chief Constable or above.

7.5. Maintenance of the System

To ensure compliance with the Information Commissioners Code of Practice and that images recorded continue to be of appropriate evidential quality The CCTV System shall be maintained under a maintenance agreement.

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

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

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

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

8. Access to and Security of Monitoring Room and Associated Equipment

8.1. Authorised use of the CCTV System

Only trained and authorised personnel will operate any of the equipment located within the CCTV monitoring room, (or equipment associated with the CCTV System). Authorised Police Officers are also permitted to use the equipment. Police officers (Guests) who are not authorised personnel may work within the control room but must not operate the CCTV System.

8.2. 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 NCP CCTV system manager. Any such visits will be conducted and recorded in accordance with the Operational Instructions.

8.3. Authorised Visits

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

8.4. Declaration of Confidentiality

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

8.5. Security

Authorised personnel will normally be present at all times when the equipment is in use. If the monitoring facility is to be left unattended for any reason it will be secured. In the event of the monitoring room having to be evacuated for safety or security reasons, the provisions of the Operational Instruction will be complied with.

The monitoring room will at all times be secured by ‘Magnetic-Locks’ operated by the restricted access control.

9. Management of Recorded Material

9.1. Guiding Principles

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

Every video or digital recording obtained by using the system has the potential of containing material that may need to be admitted in evidence at some point during the period of its retention.

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.

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

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

Recorded material will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment or otherwise made available for any use incompatible with this Code of Practice.

Information will be made available for traffic and transport monitoring, management, enforcement and information purposes

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

Every request for the release of personal data generated by this CCTV System will be channelled through the NCP CCTV System Manager or his/her representatives. The NCP CCTV System Manager will ensure the principles contained within Appendix A.3 to this Code of Practice are followed at all times.

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:

- Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in this Code of Practice;

- Access to recorded material will only take place in accordance with the standards outlined in appendix A.3 and this Code of Practice;

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

Members of law enforcement agencies having a statutory authority to investigate and / or prosecute offences may, subject to compliance with appendix A.3, release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses. This can only be done with the agreement of the NCP CCTV System Manager, in conjunction with the law enforcement agency.

If material is to be shown to witnesses, for the purpose of obtaining identification evidence, it must be shown in accordance with Appendix A.3.

It may be beneficial to make use of 'real' video footage for the training and education of those involved in the operation and management of CCTV Systems, and for those involved in the investigation, prevention and detection of crime. Any material recorded by virtue of this CCTV System will only be used for such bona fide training and education purposes.

Recorded material may be used for research purposes whereby there is a data sharing agreement in place with a university.

9.3. Recorded Material – Retention

Recorded material will be retained for a period of 31 days. All digital recording will be set to overwrite automatically.

9.4. Record of Recorded Material

Each operator has a specific user name and password for the CCTV System which maintains an audit record of all recorded material, each occasion on which that material has been accessed, retrieved, recorded or viewed.

9.5. Recording Policy

Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24-hour period in time-lapse mode, onto digital tape or digital hard drive.

Images from the CCTV Operator's main monitor can be recorded in real time, and the operators will have discretion as to which cameras are selected on the main monitor. These will usually be the incident that has the highest priority at the time.

9.6. Release of Recorded Material

If recorded material is released in accordance with this code, a record must be kept which identifies the date of release, basis for that release and to whom. Records will be retained for at least two years.

9.7. Prints of Recorded Material

Prints will be treated in the same way as other recorded information identified above. They will not be released outside the control centre except as permitted by this code, and any release will be recorded.

Where prints, which contain personal data, are taken for use within the control centre, they should not be kept for longer than can be reasonably justified, and should be regularly reviewed. Prints that are no longer required will be securely destroyed.

APPENDIX

A.1 Key Personnel and Responsibilities

1. System Owners

Bolton Council
Environmental Services
Town Hall
Victoria Sq
Bolton
BL1 1RU

Responsibilities:

Bolton Council is the 'owner' of the system. The NCP CCTV Services Manager will be the single point of reference on behalf of the owners. His/her role will include a responsibility to:

- Ensure the provision and maintenance of all equipment forming part of the System in accordance with contractual arrangements, which the owners may from time to time enter into.
- Maintain close liaison with the control room supervisor.
- Ensure the interests of the operating partners and other organisations are upheld in accordance with the terms of this Code of Practice.
- Agree to any proposed alterations and additions to the system, this Code of Practice and / or the Operational Instructions.

Operational Management

NCP CCTV Services Manager Tel: 01204 336902
Bolton Council
Town Hall
Victoria Sq
Bolton
BL1 1RU

Responsibilities*:*

- The NCP CCTV Services Manager is the 'manager' of the Bolton CCTV System
- He/she has authority for day-to-day management on behalf of the 'data controller'.
- To maintain day to day management of the system and staff;
- To accept overall responsibility for the system and for ensuring that this Code of Practice is complied with;
- To maintain direct liaison with the owners of the system and operating partners.

APPENDIX

A.2 Extracts from 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: the information constituting any personal data of which that individual is the data subject; any information available to the data controller as the source of those data; 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 to be construed as excusing the data controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by omission of names or other identifying particulars or otherwise.

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

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

Note: In considering such instances the data controller must effectively also consider the degree of privacy that the third parties might or might not reasonably expect in being at that location at that time.

(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.

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).

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

Section 8

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

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

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

(b) the data subject agrees otherwise;

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

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

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

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

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

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

APPENDIX

A.3 National Standard for the release of data to third parties

A.3.1 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 and support 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.

Bolton Council is committed to the belief that everyone has the right to respect for his or her private and family life. 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 nationally recommended standard of The CCTV User Group has been adopted by the system owners.

A.3.2 General Policy

All requests for the release of data shall be processed in accordance with the Operational Instructions. All such requests shall be channeled through the data controller or his nominated representative.

A.3.3 Primary Request To View Data

a) Primary requests to view data generated by a CCTV System are likely to be made by third parties for any one or more of the following purposes:

   i) Providing evidence in criminal proceedings;
   ii) Providing evidence in civil proceedings or tribunals
   iii) The prevention of crime
   iv) The investigation and detection of crime (may include identification of offenders)
   v) Identification of witnesses

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

   i) Police
   ii) Statutory authorities with powers to prosecute, (e.g. Customs and Excise;
   iii) Trading Standards, etc.)
   iv) Solicitors
   v) Claimants in civil proceedings
   vi) Accused persons or defendants in criminal proceedings
   vii) Other agencies, (as agreed by the Data Controller and notified to the Information Commissioner) according to purpose and legal status.

c) Upon receipt from a third party of a bona fide request for the release of data, the data controller shall:

i) Not unduly obstruct a third party investigation to verify the existence of relevant data.
ii) Ensure the retention of data which may be relevant to a request, but which may be pending application for, or the issue of, a court order or subpoena. A time limit shall be imposed on such retention, which will be notified at the time of the request.

d) Where requests fall outside the terms of disclosure and Subject Access legislation, the data controller, or nominated representative, shall:

i) Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.
ii) Treat all such enquiries with strict confidentiality.

Notes

1) 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, is required to give relevant information in writing prior to a search being granted. A charge may be made for this service to cover costs incurred. In all circumstances data will only be released for lawful and proper purposes.

2) 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.

3) The data controller shall decide which (if any) "other agencies" might be permitted access to data. Having identified those 'other agencies', such access to data will only be permitted in compliance with this Standard.

4) The data controller can refuse an individual request to view if insufficient or inaccurate information is provided. Time and date of an incident should be given to the nearest hour.

A.3.4 Secondary Request To View Data

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

i) The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. Data Protection Act 1998, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994, etc.);

ii) Any legislative requirements have been complied with, (e.g. the requirements of the Data Protection Act 1998);

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

iv) The request would pass a test of 'disclosure in the public interest'(1).

b) If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards shall be put in place before surrendering the material:

i) In respect of material to be released under the auspices of 'crime prevention', written agreement to the release of the material should be obtained from a police officer, not below the rank of Inspector. The officer should have personal knowledge of the circumstances of the crime/s to be prevented and an understanding of the CCTV System Code of Practice.

ii) If the material is to be released under the auspices of 'public well being, health or safety', written agreement to the release of material should be obtained from a senior officer within the Local Authority. The officer should have personal knowledge of the potential benefit to be derived from releasing the material and an understanding of the CCTV System Code of Practice.

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

Notes:

1) 'Disclosure in the public interest' could include the disclosure of personal data that:

i) provides specific information which would be of value to the public well being
ii) identifies a public health or safety issue
iii) leads to the prevention of crime

2) The disclosure of personal data which is the subject of a 'live' criminal investigation would always come under the terms of a primary request.

A.3.5 Individual Subject Access under Data Protection legislation

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

i) The request is made in writing;

ii) A specified fee is paid for each individual search;

iii) The data controller is supplied with sufficient information to satisfy him or her self as to the identity of the person making the request;

iv) The person making the request provides sufficient and accurate information about the time, date and place to enable the data controller to locate the information which that person seeks, (it is recognised that a person making a request is unlikely to know the precise time. Under those circumstances the council considers that within one hour of accuracy would be a reasonable requirement);

v) The person making the request is only shown information relevant to that particular search and which contains personal data of her or him self

only, unless all other individuals who may be identified from the same information have consented to the disclosure;

b) In the event of the data controller complying with a request to supply a copy of the data to the subject, only data pertaining to the individual should be copied, (all other personal data which may facilitate the identification of any other person should be concealed or erased).

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

d) In addition to the principles contained within the Data Protection legislation, the data controller should be satisfied that the data is:

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

e) A copy of the Council's 'Subject Access Request Form' along with the Council's guidance, is available at http://www.bolton.gov.uk

A.3.6 Process of Disclosure:

a) Verify the accuracy of the request.

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

c) The viewing should take place in a separate room and not in the control or monitoring area. Only data that is specific to the search request shall be shown.

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

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

APPENDIX

A.4 Restricted Access Notice

WARNING

RESTRICTED ACCESS AREA

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

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

Confidentiality Clause:

'In being permitted entry to this area you acknowledge that the precise location of the CCTV monitoring room is, and should remain, confidential. You agree not to divulge any information obtained, overheard or overseen during your visit, or use this information for any purpose other than in connection with your employment. An entry accompanied by your signature in the Visitors book is your acceptance of these terms'.

APPENDIX

A.5 Declaration of Confidentiality

The Bolton CCTV System

I, ……....., am retained by NCP Ltd to perform the duty of CCTV Control Room Operator. I have received a copy of the Code of Practice in respect of the operation and management of that CCTV System.

I hereby declare that:

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

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

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

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

Signed: ……..... Print Name: .....……

Witness: ……..... Position: .....……

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

APPENDIX

A.6 Regulation of Investigatory Powers – Guiding Principals

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

The Regulation of Investigatory Powers Act 2000 relates to surveillance by the Police and other agencies and deals in part with the use of directed covert surveillance. Section 26 of this act sets out what is Directed Surveillance. It defines this type of surveillance as:-

*Subject to subsection (6), surveillance is directed for the purposes of this Part if it is **covert** but **not intrusive** and is undertaken-*

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

(b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

(c) otherwise than by way of 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

The impact for staff CCTV monitoring centre, is that there might be cause to monitor for some time, a person or premises using the cameras. In most cases, this will fall into sub section **c** above, i.e. it will be an immediate response to events or circumstances. In this case, it would not require authorisation unless it were to continue for some time.

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

RIPA requests are authorised by a Superintendent or above. The forms must indicate the reason and should fall within one of the following categories:

An authorisation is necessary on grounds falling within this subsection if it is necessary-

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime or of preventing disorder;

(c) in the interests of the economic well-being of the United Kingdom;

(d) in the interests of public safety;

(e) for the purpose of protecting public health;

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or

(g) for any purpose (not falling within paragraphs (a) to (f)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

In cases where there is doubt as to whether an authorisation is required or not, it may be prudent to obtain the necessary authority verbally and then in writing by way of the forms. Any authority given should be recorded appropriately for later reference. This should include the name of the officer authorising.

Appendix

A.7 Behavioural Guidelines For Police Officers Operating Bolton CCTV System

Bolton Council and GMP have been working together to provide a networked CCTV solution which aims to:

1. Give authorised police officers access to live CCTV images
2. Allow control of those cameras
3. Allow access to recorded images

At this stage, view and control access is available for any of Bolton's cameras.

These guidelines have been put together to ensure that officers use the CCTV system appropriately, within the legislative framework, and in such as way that it does not compromise Bolton's responsibilities to provide a public CCTV Service.

The Purpose of the System

Bolton Council Operates a CCTV System for the following purposes:

- To assist in the detection, prevention and deterrence of crime and disorder in the area this will include:
  - Countering terrorism
  - Helping to identify, apprehend and prosecute offenders,
  - Provide the police, other agencies and the Council with evidence to take criminal and civil action in the courts
- To help reduce the fear of crime and provide reassurance to the public
- To increase public safety for those people who live, work, trade and visit Bolton
- To assist in the overall management of the public space
- To help deter and detect acts of anti-social behaviour
- To enhance community safety, assist in developing the economic well being of the Bolton area and encourage greater use of the town
- To assist in the enforcement and regulatory functions within the Bolton area
- To assist in Traffic Management
- To assist in monitoring any Emergency Planning Operations
- To assist members of the public, businesses or professional individuals with their requests for the appropriate or permitted information pertaining to incidents that may occur within the Bolton area

Circumstances in which Police many Use cameras

In certain circumstances GMP may take control of pre agreed pan, tilt, zoom (PTZ) functionality cameras, typical examples of when this may occur include:

- Direct surveillance activities agreed under the Regulation of Investigatory Powers Act.
- Specific police operations
- Day to day operations by authorised Police Officers

Prior permission for officers to use cameras should be granted by the NCP CCTV system manager.

If CCTV Operators are using the desired camera at the time of the request, then the CCTV Operator will determine which use takes priority. Cameras should NEVER be used for frivolous reasons

Only in exceptional circumstances should GMP take control of the cameras without having gained prior permission from NCP CCTV system manager.

Camera Use

The use of CCTV cameras is strictly governed by Legislation, such as the Data Protection Act, the Human Rights Act, the Protection from Harassment Act and RIPA.

All data from which people could be identified (ie shots with people in them, VRMs etc) can be classed as personal data. All personal data obtained by The CCTV System, must be processed fairly and lawfully and, in particular, shall only be processed in the exercise of achieving the objectives given above

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

Pan, Tilt & Zoom Features

All officers operating cameras should be aware that their access to the system is recorded at log on. You must not:

- ***Follow people with cameras, or excessively survey a subject for who there is no suspicion of wrongdoing unless a RIPA has been previously sought.***
- ***Use cameras to look into private residential property, unless pursuing a suspect and this is considered to be in the interests of the private residents.***

Your must never under ANY circumstances

- ***Use the cameras to look inside private domains (ie where they could legitimately consider themselves to be in a private space).***
- ***Use the cameras to look at inappropriate subjects, ie at an attractive person***
- ***Use the cameras to follow friends***
- ***Alter any system settings***

Any misuse of cameras will result in disciplinary matters.

Training and Guidance

Every person involved in the management and operation of the system will be personally issued with a copy of the Code of Practice, and will be required to sign a confirmation that they fully understand the obligations adherence to these documents places upon them and that any breach will be considered as a disciplinary offence. They will be fully conversant with the contents, 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.

All personnel involved with the system shall receive training in respect of all legislation appropriate to their role as a prerequisite for operation of cameras.

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

Security

You should never allow unauthorised officers to use the system via your log in details. To do so is to potentially compromise your own integrity, and could be illegal.

If the police monitoring facility is to be left unattended at any time, the system will be closed down so that unauthorized persons cannot gain access.

Appendix
A.8 Arrangements/Protocols with GMP

The Crime & Disorder Partnership encourages co-operation and multi agency working which has developed arrangements between Bolton Council, GMP, NCP and other and partners involved in Crime Reduction .

This Part of the Code of Practice documents the arrangements that have been agreed with these partners.

1. The Purpose

The sole purpose of this relationship is to enable NCP,Bolton Council and GMP to view, control and monitor selected CCTV data under the control of the Bolton CCTV control room and the GMP remote CCTV viewing area.

1.1 The relationship between the CCTV control room and the remote CCTV viewing area is governed by this document, which has been agreed by both NCP, Bolton Council and GMP.

2. Access to CCTV control room

All requests must comply with R.I.P.A. Act 2000 for access to carry out directed surveillance using the CCTV system and must be pre – arranged via the CCTV Control Room – 01204 336902.

1.1 Access will be authorised on production of GMP form 819b " Request for Disclosure of Personal Information " (and RIPA form if applicable) stating the requesting surveillance period, or automatic access will be given to NCP CCTV authorised Police Officers.

1.2 All resulting evidence video data will be classified as "historic data."

3. All requests for viewing historic data

2.1 All requests for disclosure of historic data on the CCTV system must be requested via the CCTV Control Room - telephone 01204 336902.

2.2 A case reference number must be obtained ,an RFD(Request for Data) number and quoted in all subsequent enquiries related to the case.

2.3 The requested data will be viewed and collated in office hours only.

2.4 Results of the requested viewing will be communicated to the requesting officer upon completion.

2.5 Disclosure will be authorised upon production of GMP 819b " Request for Disclosure of Personal Information " stating the requesting viewing period.

2.6 Evidence data shall remain available for collection for a period of no longer than 3 months. In the event of evidence data not being collected within the 3-month period, it will be destroyed in compliance with The Data Protection Act 1998, Section 1(D), Processing (d).

3. Data type

3.1 Copies of all disclosed data will be stored as case reference files on a secure Database and regularly archived (at the commencement of each calendar month).

3.2 Data will be released on (data protection format) NCP CD/DVD format. This is stand – alone and requires no additional software to operate. Full review functionality is provided including pause, variable forward / reverse replay speed, frame print, frame copy (to still image).

3.3 CD's are provided and funded by NCP. As such, The data thereon remains the responsibility of NCP CCTV system manager.

3.4 Enquiries relating to the Data Protection Act 1998 should be directed to the NCP Bolton, Town Hall, Bolton, BL1 1RU.

4. Access to the remote viewing equipment located in Bolton Central Police Station.

4.1 The system is **NOT** to be used for live image data or for retrieving recorded data during the following periods of time: - 8am to 6pm Monday through to Saturday, 6pm to 3am Thursday to Saturday and 6pm to 2am on Sunday. The system **MUST** only be used outside of these work patterns. Any attempt to do so will conflict with NCP's operating the system.

4.2 Access for users must be controlled by GMP(authorised by an Inspector) and restricted to trained operators only.

4.3 The CCTV data will be reviewed and recorded by GMP **OUT OF HOURS ONLY.**

4.4 The CCTV data viewed and collated by GMP staff is the responsibility of GMP and will fall under their data protection guidelines for Police Officers under the guidance of The Data Protection Act 1998.

5. Data Type (Remote Viewing equipment within Bolton Police Station)

5.1 Copies of all disclosed data must be stored as case reference files on a secure database and regularly archived (at the commencement of each calendar month).

5.2 Data can be released or recorded on (data protection format) CD format provided by GMP only (Bolton CCTV Control Room will not provide CD's). The recorded CD will have the ability to be stand - alone and requires no additional hardware or software to operate. Full review functionality is provided including pause, variable forward / reverse replay speed, frame print, frame copy (to still image).

5.3 The data on the CD's reviewed or recorded by GMP, remains the sole responsibility of GMP.

5.4 Enquiries relating to the recording copied data by the remote viewing equipment, located in Bolton Central Police Station, should be directed to GMP.

6. NCP's Responsibility

6.1 NCP will provide training to GMP in order to enable GMP to access and operate the remote viewing equipment.

6.2 NCP will provide an up to date DVR and Camera list for use by GMP.

6.3 NCP will respond to any system/technical issues that may arise (funding to rectify fault or replace equipment will be provided by GMP).

6.4 NCP reserves the right to withdraw the connection to the remote CCTV reviewing / recording computer should there be any deviation from the agreed protocol.

7. GMP Responsibility

7.1 GMP are solely responsible for controlling access to the remote viewing equipment and the use of video data under the guidance of The Data Protection Act 1998.

7.2 Any damage to the hardware or to the software is the sole responsibility of GMP.

7.3 Any faults or defects to the operation of the system must be reported immediately to NCP CCTV Control Room, Tel 01204 336902.