



Together in Partnership

CCTV

Code of Practice

2023

Version Control

| Version No | Date | By | Change Made |
|-------------------|---------------|-----------|-----------------------------------|
| 1.0 | January 2018 | P Bolton | Original |
| 2.0 | January 2019 | P Bolton | Review of Code of Practice |
| 3.0 | January 2020 | P Bolton | Review of Code of Practice |
| 4.0 | November 2022 | E Grundy | Amendment to the Code of Practice |
| 5.0 | August 2023 | E Grundy | Amendment to the Code of Practice |

Next Review Date November 2023

Contents

| | |
|--|----|
| Version Control | 2 |
| Definitions | 4 |
| CCTV Code of Practice | 5 |
| 1. Introduction | 5 |
| 2. Purpose of the System..... | 5 |
| 3. Operational Code of Practice | 6 |
| 4. Requests from the Media for CCTV Video Images of Crimes / Criminals..... | 7 |
| 5. Changes to This Code of Practice..... | 7 |
| 6. Responsibilities of The Operators of The System..... | 7 |
| 7. Management of the system | 8 |
| 8. Audits..... | 8 |
| 9. NCP CCTV Control Room | 8 |
| 10. Complaints Procedure | 9 |
| 11. Consultation..... | 10 |
| 12. General Data Protection Regulation & Data Protection Act 2018 – CCTV Codes of Practice | 10 |
| 13. CCTV Signs..... | 11 |
| 14. Confidentiality..... | 11 |
| 15. Human Rights..... | 11 |
| 16. Consideration Before Installation of CCTV Systems..... | 12 |
| 17. Digital Image Recording Procedures | 13 |
| 18. Disciplinary Action | 14 |
| 19. Regulation Of Investigatory Powers Act 2000 (RIPA)..... | 14 |
| 20. Protection Of Freedoms Act..... | 15 |
| 21. Freedom Of Information Act..... | 16 |
| 22. Council Directorate/Section Request To View Images | 16 |
| 23. Contact Details..... | 16 |
| Appendix 1 | 18 |
| Specific Arrangements/Protocol with GMP | 18 |
| 1. The Purpose | 18 |
| 2. Access to CCTV control room..... | 18 |
| 3. All requests for viewing historic data..... | 18 |
| 4. Data type..... | 19 |
| 5. Access to the remote viewing equipment located in Bolton Central Police Station..... | 19 |
| 6. Data Type (Remote Viewing equipment within Bolton Police Station) | 19 |
| 7. NCP's Responsibility | 20 |
| 8. GMP Responsibility | 20 |

Definitions

Authority: Bolton Council within whose boundaries the CCTV system is installed.

CCTV Strategy Meeting: Bolton Town Centre CCTV Strategy Meeting.

Partners: The term "Partners" is used to describe the working agreement between the Local Authority, Police and the Crime reduction partnership.

Police/Fire Service: Greater Manchester Police, Fire Service & Rescue Service and British Transport Police.

Owner of the System: The body having overall responsibility for the system and its operation, which is Bolton Council, Town Hall, Victoria Square, Bolton, BL1 1RU. The CCTV system is operated and maintained under a detailed Management Agreement on behalf of the Council by National Car Parks (NCP)

Data Controller: A person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which personal data are or are to be processed. In the case of Bolton Council this is the Borough Solicitor.

NCP Operations Manager: The persons responsible for the overall management of the CCTV system and operational staff.

NCP CCTV Team Leaders: The persons responsible for the day-to-day operational supervision of the CCTV Control Room.

CCTV Operators: The individuals responsible for operating the camera controls and other monitoring room equipment.

NCP Control Room: The secure area containing the CCTV monitors and the recording and editing equipment.

CCTV: Closed-Circuit Television surveillance and monitoring equipment.

The System: The Cameras with the Monitors, Recorders and Control Equipment.

Digital Time-lapse: Reduced frame rate digital recording.

D.V.R.: Digital Video Recorder.

Synectics Synergy: CCTV database and control system which is used to record all types of system faults or events monitored.

NSI: National Security Inspectorate. This organisation is a Regulatory Body for Security Organisations.

CCTV Code of Practice

1. Introduction

- 1.1. Due to the constant changes in legislation this Code of Practice will be reviewed and updated annually and will be available to the public at Bolton Town Hall and on the Council's website. It has been drawn up to govern the management of the NCP CCTV Control Room and the Authority's CCTV Public Space Surveillance System.
- 1.2. It sets out to ensure the most effective use of the system to prevent crime and disorder. It endeavours to uphold the civil liberties of those who live, work, and visit the Bolton Borough.
- 1.3. All partners who benefit from Bolton Council's CCTV system agree to be bound by this Code of Practice in order that the public interest may be best served.
- 1.4. The Code of Practice applies to all CCTV equipment linked into the Authority's Town Centre NCP CCTV Control Room.
- 1.5. It is important to state from the outset that CCTV systems will not be used as "spy systems". There will be no interest shown in or deliberate monitoring of people going about their legitimate business.
- 1.6. All digital images recorded are kept for 31 days after which they will be automatically overwritten unless an access request has been made under the following circumstances:
 - a. Police for the purpose of any criminal investigation.
 - b. Officers of Bolton Council for the purpose of any civil investigation.
 - c. Any legal obligation for access under Data Protection Legislation.
- 1.7. The release of any digital images will be in accordance with this Code of Practice and NCP CCTV Operational Manual.
- 1.8. Bolton Council's CCTV system covers 2 Town Centre areas as listed below: -
 - a. Bolton Town Centre
 - b. Farnworth Town Centre

2. Purpose of the System

- 2.1. The use of the observational CCTV system shall be for the purpose of:
 - a. Providing the Police and the Council with evidence to take criminal and civil action in the Courts;
 - b. Reducing the fear of crime and providing reassurance to the public;
 - c. Providing assistance in the detection and prevention of crime (including countering terrorism);
 - d. Assisting with the maintenance of public order;
 - e. Deterring or reducing the incidence of vandalism, graffiti, and other environmental crime;
 - f. Deterring persons from committing crimes and to enhance the opportunities for detecting those who do;

- g. Improving the safety and security of residents, visitors and the business community
- h. Discouraging anti-social behaviour including alcohol and drug-related elements;
- i. Assisting aspects of Town Centre Management.
- j. To assist in Traffic Management
- k. To assist in monitoring any Emergency Planning Operations

2.2. The Authority is committed to maintaining, reviewing, and enhancing the systems in order to ensure and improve their effectiveness. It is also committed to maintaining civil liberties.

3. Operational Code of Practice

3.1. No CCTV images shall be sold (or given) for commercial use nor made available to any person other than the Police, Fire Service, Legal profession, partner agency or Local Authority Staff (as defined in this Code of Practice), except under certain circumstances.

3.2. The circumstances referred to in Para 3.1 are as follows:

- a. The release of CCTV images to the media for commercial gain may be considered if the images shown are those of a person/persons involved in acts of crime and disorder and that any criminal investigation or criminal proceedings have concluded, and
- b. The release of CCTV images to the media does not involve the release of personal data of any individual or images of an individual who could be readily identified either by themselves or by a third party, and
- c. That agreement to release the CCTV images is supported by the Director of Place of Bolton Council, and
- d. The actual release of any CCTV images to the media will be the undertaken by the Communications and Marketing Team who will have the right to refuse the release of any images, the right to edit any images accordingly and have the responsibility of ensuring that all copyright issues are dealt with, and
- e. That there is a transparent process regarding any financial rewards received from the release of CCTV images to the media, and
- f. The financial rewards received are justified and in the interests of the economic wellbeing of Bolton Council and the public of the Borough that it represents.

3.3. Any members of the General Public who approach the Authority requesting to view the content of any CCTV images regarding any incident will be advised to report the matter to the Police for further investigation. Where a member of the public specifically asks to see CCTV images of themselves, they should be advised of the provisions under the under the General Data Protection Regulations, regarding requests for access to data.

3.4. Any requests from the Police or Fire Service for CCTV images must be made on the agreed standard form and signed by the investigating officer. The Police will also sign and accept responsibility as part of their obligations under the General Data Protection Regulations for any image released into their care.

3.5. All requests from internal Directorates for access to CCTV images must be made in writing and signed by a service Director or Assistant Director from that particular Directorate. The individual collecting the images will also sign and accept responsibility for any data released into their care.

3.6. All CCTV images provided by the Authority shall remain its property at all times and at no time is the copyright transferred to the recipient.

3.7. The Police, when required, and where operational factors allow, shall, with agreement of the Authority, have operational access to view any of the Authority's CCTV installations.

- 3.8. All CCTV images recorded shall be kept for 31 days, unless requested for the purposes stated at Para. 1.6.
- 3.9. No CCTV system shall intentionally overlook and view into private premises.

4. Requests from the Media for CCTV Video Images of Crimes / Criminals

- 4.1. CCTV images will not normally be given to the media for broadcast or reproduction. However, in exceptional circumstances, they may be provided under strict controls if it is thought that by so doing they may assist in solving a crime, but this should only be done with the express approval of all the partners and under the following conditions.
- 4.2. The General Data Protection Regulation provides that personal data should not be disclosed to third parties subject to certain exceptions, and where images from which a living individual can be identified.
- 4.3. Disclosure of CCTV images to the media for broadcasting or reproduction may be done in the following circumstances:
- a. If it would assist in the prevention or detection of crime, or the apprehension of prosecution of offenders.
 - b. If there is a reasonable belief that having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest.
 - c. Or under the circumstances referred to in Para 3.2
- 4.4. In deciding whether to disclose CCTV images to the media, a balance should be struck between the individual's right to a private / family life against the reason in (a) or (b) above for the disclosure of the information.
- 4.5. CCTV images should not be disclosed to the media unless the consent of any victim of a crime shown on the image has been first obtained wherever possible and in partnership with the Police.
- 4.6. Before any CCTV images are released to the media the advice of service management or legal services should be sought.

5. Changes to This Code of Practice

- 5.1. Minor changes to the Codes of Practice and Operational Manual that are required to efficiently maintain the Operational System may be made by the Director of Place; however, this responsibility is delegated to the NCP Operations Manager.
- 5.2. Any major changes to the Code of Practice Operational Manual will be agreed at the CCTV Strategy Meetings

6. Responsibilities of The Operators of The System

- 6.1. The Operators of the system have prime responsibility for:-

- a. Compliance with the purpose and objectives of the system;
- b. Operation and security of the system;
- c. The protection of the interests of the public and of the individual as far as is practical;
- d. The compliance with this Code of Practice;
- e. Compliance with CCTV Operational Manual;
- f. Compliance with all legislation pertaining to the use of the system.

7. Management of the system

- a. All communication between partners shall be in accordance with operational procedures in force at the time.
- b. Any video links between the CCTV Control Room and the Police shall be used only in accordance with agreed operational procedures.

7.1. Access to Resources

Arrangements for access to recordings and the CCTV control room shall follow this Code of Practice

8. Audits

- 8.1. There will be regular internal 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.
- 8.2. Bi-annual audits will be undertaken by the NSI to ensure the NCP CCTV monitoring facilities are in full compliance with BS7958, BS7858 and BS EN ISO 9001.

9. NCP CCTV Control Room

9.1. Access to and Security of the CCTV Control Room

- a. Access to view monitors, whether to operate the equipment or to view the images, is limited to authorised staff with that responsibility.
- b. Only authorised personnel are to be admitted to the control room. The names of all authorised personnel are held within both the control room access control system and the service operational manual and all such staff must carry an official identification card.
- c. Visits by non-authorised personnel for example, Councillors, Council employees or the Police can only be authorised by the Director of Place. However, this responsibility is delegated to the NCP Operations Manager.
- d. Visitors will only be allowed access to the control room if the visit has been authorised in advance. An authorised member of staff must accompany all visitors

and ensure that they sign in the visitor's book before entering and exiting the control room.

- e. Access to or the display of monitors shall not be allowed except for lawful, proper and sufficient reasons and, on such occasions, adequate precautions shall be in place to ensure security and privacy of individuals and information.

9.2. Operational Standards

- a. The CCTV control room shall operate to a recognised "NSI Gold Standard" ensuring that "best practice" and strict security procedures are maintained.
- b. All control room staff shall undergo Greater Manchester Police Non Police Personnel Vetting, Disclosure and Barring Service enhanced check and checks in accordance to BS7858.
- c. All control room staff shall be trained accordingly and licensed by the Security Industry Authority (SIA)
- d. The CCTV Control Room shall facilitate camera operation, viewing, monitoring and constant recording of CCTV installations.

10. Complaints Procedure

- 10.1. The Council has an existing Complaints Procedure, copies of which are available from:

Bolton Town Hall,
Victoria Square, Bolton,
BL1 1RU,
Tel. No. 01204 333333
Website: www.bolton.gov.uk
Email CCCGroup@bolton.gov.uk

- 10.2. This procedure must be used for any complaints regarding Town Centre CCTV owned by the Council.

- 10.3. The salient points of the Complaints Procedure are:-

- a. Complaints to the Council should be made within a reasonable time frame of the event which caused the complaint to occur. In most cases 12 months is regarded as the appropriate limitation period.
- b. All written complaints will be acknowledged within five working days (24 hours for emails), a full response will be provided within 20 working days but if we are unable to reply within this time, we will contact you and let you know the reason why and tell you when you can expect a full response.
- c. If you are not satisfied with the response, you will have the opportunity to appeal in writing within 28 calendar days to the Chief Executive. The complaint will be reviewed by the Departmental Monitoring Officer in consultation with the Departmental Director.
- d. Any complaints received against the Police must be forwarded immediately to the Divisional Chief Superintendent based at Bolton Divisional Police Headquarters, to be dealt with through normal Police procedures.
- e. You have the right to complain to the Information Commissionaires Office at the following address:

Information Commissioners Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire SK9 5AF.

11. Consultation

- 11.1. Bolton Council works in Partnership and prides itself on its participation, co-operation, and communication with all interested parties in the fight to prevent and reduce crime.
- 11.2. A consultation strategy for CCTV installations must be adhered to for any new installations or system alterations.
- 11.3. The salient points of the consultation strategy are:-
 - a. Any proposed CCTV system must be the subject of adequate research and consultation within the area to be covered by the camera system and where applicable the adjacent areas.
 - b. No CCTV system will be considered unless it has the Council and Divisional Police Command support.
 - c. If there are unresolved difficulties with any consultation process, then refer to the CCTV Strategy meeting for advice.
 - d. A CCTV System must not infringe legislation on human rights issues, i.e. privacy and this must be explained as part of the consultation process.
 - e. All parties involved must be informed about the provisions relating to CCTV contained in the General Data Protection Regulation and the Data Protection Act – CCTV Codes of Practice.

12. General Data Protection Regulation & Data Protection Act 2018 – CCTV Codes of Practice

- 12.1. The Authority has an obligation to comply with the requirements of the General Data Protection Regulations and Data Protection Act 2018, as such the data controller is registered for use of CCTV, Bolton Council's registration number is Z6659663.
- 12.2. All CCTV Systems which record pictures should be registered under the General Data Protection Regulation. The Regulation contains a process for people to have access to video recordings under defined conditions. (Below is a brief summary of the provisions of the Act).
- 12.3. The General Data Protection Regulation provides that where an application is made in writing to the Data Controller (D.C.), an individual is entitled to be informed of the following detail:
 - a. Confirmation that their data is being processed
 - b. Access to their personal data, and
 - c. Other supplementary information

- 12.4. The D.C. must also provide the information which forms the personal data, eg. a copy of the recordings.
- 12.5. Should other persons be identifiable, then consent should normally first be obtained from them before disclosure is made, unless having regard to all the circumstances, it is reasonable to disclose the data without the second individual's consent.
- 12.6. There is an exception to this which covers personal data processed for the purpose of the prevention or detection of crime or the apprehension or prosecution of offenders, which might be prejudiced by disclosure of the data.
- 12.7. In addition, the Act also requires appropriate steps to be taken to avoid unauthorised or unlawful processing. Apart from data subjects, access to recorded images is therefore limited.
- 12.8. If a person requests video images of themselves a request for access to data form needs to be completed by the applicant (forms can be obtained via the Council website).
- 12.9. Appeals – if an individual believes that a Data Controller has failed to comply with a request for access to data in contravention of the Act, they may apply to Court for an order that the Data Controller complies with the request. Other appeals can be forwarded to:

the Information Commissioners Office
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire
SK9 5AF.

13. CCTV Signs

- 13.1. All CCTV systems shall have appropriate signage in accordance with the Data Protection Act 2018, advising people that CCTV is in operation. These signs need to be placed on the perimeter of the CCTV system and other strategic places.
- 13.2. The CCTV signs will vary in size according to location and the circumstances. Each sign shall contain the identity of the organisation responsible for the scheme and its purpose. A contact number should be given for further information about the scheme.
- 13.3. If signs are to be installed on public highways, then permission and advice on locations must be sought from the Director of Place, Directorate.

14. Confidentiality

- 14.1. CCTV images may contain sensitive scenes and information; therefore, confidentiality must be maintained at all times. It is essential that strict security is maintained and access to images restricted. (For exceptions see Para 1.6).

15. Human Rights

- 15.1. All CCTV systems in their design, management and operation must comply with Human Rights Legislation.

15.2. 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.

15.3. 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.

15.4. The Bolton CCTV System shall be operated with respect for all individuals, recognising 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.

15.5. 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.

15.6. 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.

16. Consideration Before Installation of CCTV Systems

16.1. In considering the installation of a CCTV System, we will ensure that it complies with the Authority's Code of Practice and in so doing, prior to purchase, satisfy its requirements on:

- a. The purpose of the CCTV system with evidence to suggest its introduction will satisfy the demand.
- b. The CCTV systems purpose linked with other crime prevention measures.
- c. The adequacy of the procedures for System Management.

16.2. In the likely event that CCTV recorded images are to be used as Court evidence, the following questions should be considered:

- a. What level of detail is the camera expected to identify, e.g. groups of people, individuals, car number plates etc?
- b. What operational requirements are needed, i.e., night-time efficiency (there are 4000 hours of darkness per annum), number of cameras, colour or monochrome, the frequency of time-lapse recording etc.
- c. Consider measures to protect the CCTV cameras from vandalism.
- d. Can the subsequent revenue costs for running the system be afforded?

16.3. Further Information

Useful information can be obtained by browsing the Home Office web site www.homeoffice.gov.uk and the Information Commissioners Office web site www.ico.gov.uk.

16.4. The Home Office has provided a number of informative documents some of which are as follows:

- a. CCTV – Looking Out for You
- b. CCTV Operational Requirements Manual
- c. National CCTV Strategy
- d. Surveillance Camera Code of Practice

16.5. There are other useful sources of information:

- a. The British Security Industry Association has published a "User Guide to CCTV Systems Performance"
- b. The Local Government Association
- c. The Home Office Scientific Development Branch

17. Digital Image Recording Procedures

17.1. Adhering to the agreed management and operational procedures is crucial if the digital recordings produced are to be of sufficient evidential value and quality that they can be used for intelligence gathering purposes or as evidence to be produced in a court.

17.2. Time lapsed digital images are automatically recorded and are kept for 31 days on the hard drive of the recording equipment, after which the images will be overwritten. Any images retained beyond the 31 days should be archived and retained for no longer than 5 years, after which all images should be deleted manually by the appropriate nominated officer.

17.3. For evidential purposes each recorded image downloaded should have the correct time and date automatically embossed on it, therefore it is essential that operators periodically check that images released are correct.

17.4. If a request for access to recorded images is made within the 31 days, then only copies of the images that have been specifically requested can be downloaded. These images can be downloaded on either DVD or CD-ROM formats.

17.5. Each recorded image that is released should be endorsed with all relevant information pertaining to what the image relates to and any FWIN report numbers.

17.6. Digital Recording Viewing/Copying Procedure

On receiving a request to view a digital recording of a particular incident, the following process should be followed:

- a. To preserve the continuity of evidence a report should be created on the Synectics Synergy database for either a viewing or a copy made of a digital recording, thereby creating a unique incident reference number.
- b. The report should include the following:

- The name, rank or title of the person requesting the viewing or copy,
 - The organisation that the person represents, Incident type e.g. assault theft etc,
 - Date time and location of the incident,
 - Police/Fire Service FWIN (if applicable)
 - Copy of the relevant Police form.
 - Any additional information applicable
- c. Each digital image recording released should be clearly identified with the relevant incident report number, start and finish time, date of the incident and the Police/Fire Service FWIN (if applicable).
- d. It is important to stress to the recipient of digital image recordings that the images will at all times remain the copyright property of Bolton Council. Therefore no images should be released either wholly or partially to a third party without the written consent from Bolton Council. A record of all data released will be kept by the Authority for 5 years.

18. Disciplinary Action

18.1. The appropriate disciplinary action should be implemented where there is a deliberate breach of security procedures (or this Code of Practice) and staff should be made aware of such disciplinary procedures.

19. Regulation Of Investigatory Powers Act 2000 (RIPA)

19.1. 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

19.2. The impact for staff in the 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.

19.3. 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.

19.4. 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.

19.5. 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.

19.6. When another agency (e.g. Police, HM revenue & Customs etc) wish to use the NCP/Bolton Council's physical resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any officer agrees to allow the NCP/Council's resources to be used for the other agency's purposes, they must obtain a copy of that agency's RIPA form for the record or relevant extracts from the same which are sufficient for the purposes of protecting NCP/Council and the use of its resources. A copy should be made of the material obtained and passed to the CCTV Supervisor for inclusion in the CCTV RIPA Evidence Locker.

Under the Directed surveillance crime threshold amendments: NCP/Bolton Council will only grant an authorisation under RIPA for the use of directed surveillance where it is investigating criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco.

Copies of the Home Office's Codes of Practice can be viewed on their website: www.gov.uk/government/organisations/home-office/series/ripa-codes and the OSC website: <http://surveillancecommissioners.independent.gov.uk>

19.7. All RIPA and Non-RIPA authorisation wishing to utilise the Town Centre CCTV system must meet the requirements as contained in the Bolton Council RIPA Policy and Guidance document.

20. Protection Of Freedoms Act

20.1. A new Surveillance Camera Code of Practice came into force on 4th June 2013 and operates supplementary to existing legislation and the ICO CCTV Code of Practice. The Code is pursuant to Section 29 of the Protection of Freedoms Act 2012.

NCP/Bolton Council will operate in full compliance with this new legislation and has incorporated beneath 12 guiding principles as contained within the Protection of Freedoms Act 2012:

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

21. Freedom Of Information Act

- 21.1. It is essential that before releasing any data under a Freedom of Information request that advice should be sought from the Authorities Legal Services, also information relating to this subject can be found on the Authorities internet/intranet:

<http://www.bolton.gov.uk/website/pages/FreedomofInformation.aspx>

22. Council Directorate/Section Request To View Images

- 22.1. Any other Council Directorate/Section may request to view CCTV images in pursuit of any alleged criminal or civil action, the procedure for access is at (Para 3.5)

23. Contact Details

Data Controller:
Bolton Town Hall,
Victoria Square,

Bolton,
BL1 1RU,
Tel. No. 01204 333333
Website www.bolton.gov.uk.

The CCTV data protection officer:
NCP Operations Manager,
Bolton Council/NCP CCTV Control Room,
Town Hall,
Victoria Square, Bolton,
BL1 1RU,
Tel No. 01204 336902.

Appendix 1

Specific Arrangements/Protocol 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 this partner.

1. The Purpose

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

2. Access to CCTV control room

- 2.1. 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 – Tel 01204 336902.
- 2.2. Access will be authorised on production of GMP form “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.
- 2.3. All resulting evidence video data will be classified as “historic data.”

3. All requests for viewing historic data

- 3.1. All requests for disclosure of historic data on the CCTV system must requested via the CCTV Control Room - telephone 01204 336902.
- 3.2. A case reference number must be obtained an RFD (Request for Data) number and quoted in all subsequent enquiries related to the case.
- 3.3. The requested data will be viewed and collated in office hours only.
- 3.4. Results of the requested viewing will be communicated to the requesting officer upon completion.
- 3.5. Disclosure will be authorised upon production of GMP form “Request for Disclosure of Personal Information “stating the requesting viewing period.
- 3.6. Evidence data shall remain available for collection from Solicitors and GMP for a period of no longer than 6 months. In the event of evidence data not being collected within the 6-month period, it will be destroyed in compliance with the General Data Protection Regulation.

4. Data type

24.

- 4.1. Copies of all disclosed data will be stored as case reference files on a secure Synectics Synergy database and regularly archived (at the commencement of each calendar month).
- 4.2. Data will be released on (data protection format) NCP CD/DVD format. This is stand-alone and requires no additional software to open. Full review functionality is provided including pause, variable forward / reverse replay speed, frame print, frame copy (to still image).
- 4.3. CD's/DVD are provided and funded by NCP. As such, the data thereon remains the responsibility of NCP Operations Manager.
- 4.4. Enquiries relating to the General Data Protection Regulation should be directed to the Bolton Council Information Governance Team, Town Hall, Bolton, BL1 1RU.

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

- 5.1. The system allows access to live and recorded CCTV data within Bolton Central Police station. The remote viewing systems primary use is to allow access to CCTV images and recordings outside the operational hours of the NCP CCTV control room, but may also be used at any time during an emergency situation. Primacy of control of the CCTV system is at all times with the NCP CCTV Control Room.
- 5.2. Access for users must be controlled by GMP (authorised by an Inspector) and restricted to trained operators only. Access to the system is password protected and only trained staff should be issued with the password.
- 5.3. The Synectics Synergy CCTV system logs all actions taken on the CCTV system and details of all requests for data and CD's/DVD produced by the police. This system is fully auditable for control room management.
- 5.4. 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 General Data Protection Regulation.

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

- 6.1. Copies of all disclosed data must be stored as case reference files on a secure Synectics Synergy database.
- 6.2. Data can be released or recorded on (data protection format) CD/DVD format provided by GMP only (Bolton CCTV Control Room will not provide CD's/DVD). The recorded CD/DVD 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).
- 6.3. The data on the CD's/DVD reviewed or recorded by GMP remains the sole responsibility of GMP.
- 6.4. Enquiries relating to the recording copied data by the remote viewing equipment, located in Bolton Central Police Station, should be directed to GMP.

7. NCP's Responsibility

- 7.1. NCP will provide training to GMP in order to enable GMP to access and operate the remote viewing equipment.
- 7.2. NCP will provide an up to date Camera list for use by GMP.
- 7.3. NCP will respond to any system/technical issues that may arise (funding to rectify fault or replace equipment will be provided by GMP).
- 7.4. NCP reserves the right to withdraw the connection to the remote CCTV reviewing / recording computer should there be any deviation from the agreed protocol.

8. GMP Responsibility

- 8.1. GMP is solely responsible for controlling access to the remote viewing equipment and the use of video data under the guidance of the General Data Protection Regulation.
- 8.2. Any damage to the hardware or to the software is the sole responsibility of GMP.
- 8.3. Any faults or defects to the operation of the system must be reported immediately to CCTV Control Room, Tel 01204 336902.