Warrington Borough Council

in partnership with

Cheshire Constabulary

Code of Practice

for the operation of

Closed Circuit Television

Update April 2020

Warrington Borough Council

CONTENTS

Section 1 Introduction and Objectives

1.1 Introduction

A Closed Circuit Television (CCTV) system is in operation in Warrington Town Centre. This system, known as Warrington CCTV, comprises a number of cameras installed at strategic locations. The cameras are fully operational with pan, tilt and zoom facilities and are monitored from the Council's purpose built Control Room. Secondary monitoring facilities are located at the Cheshire Constabulary Police Headquarters, Winsford.
For the purposes of this document, the 'owner' of the system is Warrington Borough Council.
For the purposes of the Data protection Act 2018 and the General Data Protection Regulation (GDPR) the 'data controller' is Warrington Borough Council (Note 1.).
The Data Protection (charges and Information) Regulations 2018 requires every organisation that processes personal information to pay a fee to the Information Commissioner's office (ICO). Warrington Borough Council is registered with the Information Comissioners office and its registration number is Z4794892.
Details of key personnel, their responsibilities and contact points are shown at appendix A to this Code.

*Note1. The **data controller** is the person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data are to be processed. It must be a legal entity e.g. person, organisation or corporate body and in the case of partnerships all partners may be considered to bear the responsibility.*

1.2 Partnership statement in respect of The Human Rights Act 1998

1.2.1 The partnership 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, and consider that the use of CCTV in Warrington is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety.

1.2.2 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 and it is also considered a necessary initiative by the Partnership towards their duty under the Crime and Disorder Act 1998.

1.2.3 It is recognised that operation of the Warrington CCTV System may be considered to infringe on the privacy of individuals. The partnership recognise 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.

1.2.4 The Codes of Practice shall ensure that evidence is secured, retained and made available as required to ensure there is absolute respect for everyone's right to a free trial.

1.2.5 The Warrington 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.

1.3 Objectives of the System

1.3.1 The objectives of the Warrington CCTV System as determined by the Partnership which form the lawful basis for the processing of data are:-

- *To help reduce the fear of crime and anti-social behaviour*
- *To help deter crime and anti-social behaviour*
- *To help identify, apprehend and prosecute offenders.*
- *To help detect crime and provide evidential material for court proceedings*
- *To assist in the overall management of Warrington Town Centre*
- *To help secure a safer environment for those who live, work, trade in and visit the area*
- *To enhance community safety and therefore assist in developing the economic well being of Warrington Town Centre and encourage greater use of its facilities*
- *To assist the Local Authority in its enforcement and regulatory functions.*
- *To assist in the effective and efficient deployment of resources*

Section 2 Statement of Purpose and Principles

2.1 Purpose

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

2.21 General Principles of Operation

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

2.2.2 The operation of the system will also recognise the need for formal authorisation of any covert surveillance that falls within the definition of 'Directed Surveillance' under the Regulation of Investigatory Powers Act 2000 (see Appendix F).

2.1.1 The system will be operated in accordance with the DPA 2018 and GDPR at all times.

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

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

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

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

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

2.3 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

2.4.1 The areas covered by CCTV to which this Code of Practice refers are the public areas within the responsibility of the operating partners and cover the Warrington Town Centre area.

2.4.2 From time to time transportable or mobile cameras may be temporarily sited within the area. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the CCTV System and be governed by these Codes and Procedures.

2.4.3 The cameras are all HD with a pan tilt and zoom (PTZ) operation.

2.4.4 None of the cameras forming part of the System will be installed in a covert manner. The presence of CCTV cameras are identified by signs.

2.4.5 A map showing the number and location of all fixed cameras is available for inspection.

2.5 Monitoring and Recording Facilities

2.5.1 A staffed monitoring room is located at the Warrington Borough Council CCTV Control Room. The CCTV equipment has the capability of recording all cameras simultaneously throughout every 24 hour period.

2.5.2 Secondary monitoring equipment is sited at Cheshire Police HQ for viewing only. No equipment, other than that housed within the main CCTV control room shall be capable of recording images from any of the cameras.

2.5.3 CCTV operators are able to record images from selected cameras in real-time, produce DVD's of recorded images, replay or copy any pre-recorded data at their discretion and in accordance with the Code of Practice. All viewing and recording equipment shall only be operated by trained and authorised users.

2.6 Human Resources

2.6.1 Unauthorised persons will not have access to the CCTV Control Room without an authorised member of staff being present.

2.6.2 The monitoring room shall be staffed by specially selected and trained operators.

2.6.2 All operators shall receive training relevant to their role in the requirements of the Human Rights Act 1998,the Data Protection Act 2018, GDPR, Regulation of Investigatory Powers Act 2000 and the Codes of Practice and Procedures. Further training will be provided as necessary.

2.7 Processing and Handling of Recorded Material

2.7.1 All recorded material will be processed and handled strictly in accordance with this Code of Practice.

2.8 Operators Instructions

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

2.9 Changes to the Code.

2.9.1 Any major changes to the Code of Practice (i.e. such as will have a significant impact upon the Code of Practice or upon the operation of the system) will take place only after consultation with, and upon the agreement of all organisations with a participatory role in the operation of the system.

2.9.2 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 manager and the owners of the system.

Section 3 Privacy and Data Protection

3.1 Public Concern

3.1.1 Although the majority of the public at large may have become accustomed to the use of CCTV cameras, those who do express concern do so mainly over matters pertaining to the processing of the information, (or data) i.e. what happens to the material that is obtained.

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

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

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

3.1.3 The storage and security of the data will be strictly in accordance with the requirements of GDPR and additional locally agreed procedures.

3.2 Data Protection Legislation

3.2.1 Warrington Borough Council is registered with the Information Commisioners office and its registration number is Z4794892.

3.2.2 The 'data controller' for The System' is Warrington Borough Council and day to day responsibility for the data will be devolved to the CCTV Manager.

3.2.3 All data will be processed in accordance with the principles of Article 5 of the General Data Protection Regulation (GDPR)

Article 5 (1) requires that personal data shall be;

1) Processed lawfully, fairly and in a transparent manner.
2) Collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with these purposes.
3) Adequate, relevant and limited to what is necessary in relation to the purposes in which they are processed.
4) Accurate and where necessary, kept up to date and where inaccurate, erased or rectified without delay.
5) Kept in a form which permits identification of date subjects for no longer than is necessary for the purpose.
6) Processed in a manner that ensures appropriate security of the data.

3.3 Rights of the individual

The GDPR provides the following rights for individuals;

1) The right to be informed
2) The right of access (also known as subject access)
3) The right to rectification
4) The right to erasure
5) The right to restrict processing
6) The right to data portability
7) The right to object
8) Rights in relation to automated decision making and profiling

The rights available to each individual depends on the reason for processing your information. As not every right will apply, requests will be reviewed on a case by case basis.

3.4 Request for information (subject access)

3.4.1 Any request from an individual for the disclosure of personal data which he/she believes is recorded by virtue of the system, will be directed in the first instance to the system manager or data controller via the councils formal subject access request process.

3.4.1 If the request cannot be complied with without identifying another individual appropriate redaction or pixilation will be completed where appropriate.

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

Section 4 Accountability and Public Information

4.1 The Public

4.1.1 For reasons of security and confidentiality, access to the CCTV monitoring room is restricted in accordance with this Code of Practice. However, in the interest of openness and accountability, Partners wishing to visit the room may be permitted to do so, subject to the approval of, and after making prior arrangements with the CCTV management.

4.1.2 Cameras will not be used to look into private residential property. 'Privacy zones' are programmed into the system as required in order to ensure that the interior of any private residential property within range of the system is not surveyed by the cameras.

All complaints shall be dealt with in accordance with Warrington Borough Council's complaints procedure, a copy of which may be obtained from the Warrington Borough website. Any performance issues identified will be considered under the organisations disciplinary procedures to which all members of Warrington Borough Council, including CCTV personnel, are subject.

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

4.2 System Owner

4.2.1 The Director of Economic Regeneration, Growth and Environment being the nominated representative of the system owner

4.2.2 Formal consultation will take place between the owners and the managers of the system and relevant partners, with regard to all aspects, including this Code of Practice.

4.3 System Manager

4.3.1 The nominated manager named at appendix A will have day-to-day responsibility for the system as a whole.

4.3.2 The system manager will ensure that every complaint is acknowledged and a written response issued.

4.4 System Development

4.4.1 Any major technological changes which may significantly affect the operation of the System will be fully assessed in relation to the purpose and objectives of the scheme.

4.4.2 Consultation with all partners will take place before the introduction of the aforementioned changes.

4.5 Public Information

4.5.1 Code of Practice

A copy of the CCTV Code of Practice shall be published on the Warrington Borough Council web site.

4.5.2 Signs

Signs (as shown below) will be placed in the locality of the cameras. The signs will indicate:

i) The presence and the purpose of the CCTV monitoring;

ii) The 'ownership' of the system;

iii) Contact telephone number.

Section 5 Assessment of the System and Code of Practice

5.1 Evaluation

The System can be independently evaluated to establish whether the purposes of the system are being complied with and to assess the number of incidents, type of incidents and the number of requests that are dealt with.

The results of the evaluation will be used to review and develop any alterations to the specified purpose and objectives of the scheme as well as the functioning, management and operation of the system.

5.2 Monitoring

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

The 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

5.3 Audit

Audits, which may be in the form of irregular spot checks, will include examination of the CCTV record logs, recorded material and photograph logs.

Section 6 Human Resources

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

6.1.1 The CCTV Monitoring Room will be staffed in accordance with Warrington Borough Council's recruitment and selection policies. 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. All CCTV staff will be vetted by Cheshire Constabulary every 3 years.

6.1.2 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 which adherence to this document places upon them and that any breach will be considered as a disciplinary offence. They will be fully conversant with the contents of the document.

6.1.3 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

6.2.1 Every individual with any responsibility under the terms of this Code of Practice and who has any involvement with The System to which they refer, will be subject to the employing Authority discipline code. Any breach of this Code of Practice or of any aspect of confidentiality will be dealt with in accordance with those discipline rules.

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

6.3 Declaration of Confidentiality

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

Section 7 Control and Operation of Cameras

7.1 Guiding Principles

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

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

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

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

7.1.5 Camera operators will be mindful of exercising prejudices 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 system manager.

7.2 Primary Control

7.2.1 Only those trained and authorised members of staff with responsibility for using the CCTV equipment will have access to the operating controls, those operators have primacy of control at all times.

7.3 Secondary Control

7.3.1 No secondary control facilities are installed.

7.4 Operation of The System by the Police

7.4.1 Under extreme circumstances the Police may make a request to assume direction of The System to which this Code of Practice applies. Only requests made on the written authority of a police officer not below the rank of Superintendent will be considered. Any such request will only be accommodated on the personal written authority of the most senior representative of the System owners, or designated deputy of equal standing. Any request and approval referred to above will be accepted either verbally or in writing. A verbal request or approval will be supported in writing as soon as reasonably practicable.

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

7.5 Maintenance of the system

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

7.5.2 The maintenance agreement will make provision for regular/ periodic service checks on the equipment which will include cleaning of camera's, ensure wipers are working and checks on the functioning of the equipment

7.5.3 The maintenance will also include the replacement of equipment which is reaching the end of its serviceable life.

7.5.4 The maintenance contract provides a 24 hour help desk for reporting faults.

7.5.5 The maintenance agreement will define the maximum periods of time permitted for attendance by the engineer and for rectification of the problem depending upon the severity of the event and the operational requirements of that element of the system.

7.5.6 It is the responsibility of the CCTV Team Leader to ensure appropriate records are maintained in respect of the functioning of the cameras and the response of the maintenance organisation.

Section 8 Access to, and Security of, the Operations Centre and Associated Equipment

8.1 Authorised Access

8.1.1 Only trained and authorised personnel will operate any of the equipment located within the CCTV monitoring room, (or equipment associated with the CCTV System).

8.2 Public access

8.2.1 Public access to the monitoring and recording facility is prohibited.

8.3 Authorised Visits

8.3.1 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

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

8.5 Security

8.5.1 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.

8.5.2 The monitoring room will at all times be secured by key fob entry, with access only to authorised CCTV staff.

Section 9 Management of Recorded Material

9.1 Guiding Principles

9.1.1 For the purposes of this Code 'recorded material' means any material recorded by, or as the result of, technical equipment which forms part of The System, but specifically includes images recorded digitally, images stored on DVD and still photographs.

9.1.2 Every digital recording obtained by using The System has the potential of containing material that has to be admitted in evidence at some point during its life span.

9.1.3 Members of the community must have total confidence that information recorded about their ordinary-every-day activities by virtue of The System, will be treated with due regard to their individual right to respect for their private and family life.

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

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

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

9.2 Release of data to a third party

9.2.1 Every request for the release of personal data generated by this CCTV System will be channelled through the System Manager/CCTV Team Leader, who will ensure the principles contained within Appendix B to this Code of Practice are followed at all times.

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

- 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 B and this Code of Practice;
- The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

9.2.3 Members of the police service or other agency having a statutory authority to investigate and/or prosecute offences may, subject to compliance with appendix C, release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses.

9.2.4 If material is to be shown to witnesses, including police officers, for the purpose of obtaining identification evidence, it must be shown in accordance with Appendix C.

9.2.5 It may be beneficial to make use of 'real' 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 will not be released for commercial or entertainment purposes.

9.3 Data Discs - Provision & Quality

9.3.1 To ensure the quality of the data, and that recorded information will meet the criteria outlined by current Home Office guidelines, the only data discs (DVD's) to be used with the system are those which have been supplied by Cheshire Police.

9.4 Retention

9.4.1 Recorded data will be stored on the hard drive for a period of 30 days and will then be automatically deleted. If retained it will be held on the system hard drive or on data discs (DVD). Once information is no longer required it will be deleted, or the discs shredded, immediately.

9.4.2 Discs will always be used and stored in accordance with the System manufacturer's and the supplier's recommendations. After a period of three years they will be destroyed and the destruction certified.

9.5 Disc Register

9.5.1 Each disc or digitally stored image will have a unique tracking record number. The tracking record shall identify the person who has requested the footage to be retained on the hard drive or burnt to a disc and for what purpose. There is a signing out record for each disc that has been issued.

9.6 Recording Policy

9.6.1 Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24 hour period.

9.7 Evidential Discs

9.7.1 In the event of a disc being required for evidential purposes the procedures outlined above will be strictly complied with.

Section 10 Image Prints

10.1 Guiding Principles

10.1.1 An image print is a copy of an image or images which already exist on hard drive or disc. Such prints are equally within the definitions of 'data' and recorded material

10.1.2 Image prints will not be taken as a matter of routine. Each time a print is made it must be capable of justification by the originator who will be responsible for recording the full circumstances under which the print is taken.

10.1.3 Image prints contain data and will therefore only be released under the terms of Appendix B to this Code of Practice, 'Release of data to third parties'.

10.1.4 A record will be maintained of all image print productions. The recorded details will include: a sequential number, the date, time and location of the incident, date and time of the production of the print and the identity of the person requesting the print and will be signed out on request to the police.

10.1.5 The records of the image prints taken will be subject to audit in common with all other records in the system.

Appendix A Key Personnel and Responsibilities

1. System Owners

Warrington Borough Council
Town Hall
Sankey St.
Warrington

Tel: 01925 440000

Responsibilities:

Warrington Borough Council is the 'owner' of the system. The CCTV Manager will be the single point of reference on behalf of the owners with responsibility to:

i) Ensure the provision and maintenance of all equipment forming part of the Warrington CCTV System in accordance with contractual arrangements

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

i) Agree to any proposed alterations and additions to the system or this Code of Practice.

System Management

Deputy Chief Executive and Director of corporate services
Warrington Borough Council

CCTV, UTMC and Parking Services Manager
Warrington Borough Council

CCTV Team Leader
Warrington Borough Council

Responsibilities*:*

The CCTV Manager/Team Leader has delegated authority for data control on behalf of the 'data controller'.
This role includes responsibility to:

i) Maintain day to day management of the system and staff.

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

iii) Maintain direct liaison with the owners of the system/operating partners.

Appendix B National Standard for the release of data to third parties

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.

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

2. General Policy

All requests for the release of data shall be processed in accordance with this Code of Practice. All such requests shall be channelled through the data controller although day to day responsibility may be devolved to the System Manager.

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 investigations or proceedings
   ii) Providing evidence in civil proceedings or tribunals but only where directly affecting the Council.
   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 investigate and prosecute, (e.g. Customs and Excise; Trading Standards, etc.)
   iii) Solicitors
   iv) Insurance companies.

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) In circumstances outlined at note (3) below, (requests by plaintiffs, accused persons or defendants) the data controller, or nominated representative shall:

i) Be satisfied that there is no inconsistency with any data held by the police in connection with the same investigation.
ii) All such enquiries are to be processed by all parties in accordance with the Data Protection Act 2018.

Notes

(1) The release of data to the police is not be restricted to the civil police but could include, (for example) British Transport Police, Ministry of Defence Police, Military Police, etc.

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

(3) There may be occasions when an enquiry by a plaintiff, an accused person, a defendant or a defence solicitor falls outside the terms of disclosure or subject access legislation. An example could be the investigation of an alibi. Such an enquiry may not form part of a prosecution investigation. Defence enquiries could also arise in a case where there appeared to be no recorded evidence in a prosecution investigation.

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

(5) The data controller can refuse an individual request to view if insufficient or inaccurate information is provided. A search request should specify reasonable accuracy (could be specified to the nearest ½ hour).

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 2018, GDPR, 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 2018,GDPR)

   iii) Due regard has been taken of any known case law (current or past) which may be relevant

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

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

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

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

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

4. Individual Subject Access under Data Protection legislation

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

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

2) The person making the request provides sufficient and accurate information about the time, date and place to enable the data controller to locate the

information which that person seeks, (it is recognised that a person making a request is unlikely to know the precise time. Under those circumstances it is suggested that within one hour of accuracy would be a reasonable requirement)

3) 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;

v) For individual disclosure only (i.e. to be disclosed to a named subject)

5. Process of Disclosure:

a) Verify the accuracy of the request.

b) A SAR form to be completed (see Appendix E) where possible to provide an audit trail of the request.

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

d) It must not be possible to identify any other individual from the information being shown, (any such information will be blanked-out using privacy masking/pixilation or redaction.

6. Media disclosure

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

i) The release of the material must be accompanied by a signed release document that clearly states what the data will be used for and sets out the limits on its use.

ii) The release form shall state that the receiver must process the data in a manner prescribed by the data controller, e.g. specific identities/data that must not be revealed.

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

iv) The release form shall be considered a contract and signed by both parties**.**

7. Principles

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

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

b) Access to recorded material shall only take place in accordance with this Standard and the Code of Practice;

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

Appendix C Restricted Access Notice

WARNING

RESTRICTED ACCESS AREA

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

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

Confidentiality Clause:

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

Appendix D Declaration of Confidentiality

The Warrington CCTV System

I, ……....., am retained by Warrington Borough Council to perform the duty of CCTV Control Room……. 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 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 Warrington Borough Council may be an offence against the Official Secrets Act of 1911, Section 2, as amended by the Official Secrets Act of 1989.

Signed: …… Print Name: ……

Witness: …….. Position: ……..

Dated this ……..day of……. (month) 20

Appendix E Subject Access Request Form

SUBJECT ACCESS APPLICATION FORM CCTV (DATA PROTECTION ACT 2018)

This form is to be used when an individual (the data subject), or authorised representative wishes to access personal data held by Warrington Borough Council.

<table>
<tr><td colspan="2">Please complete in BLOCK CAPITALS – illegible forms will delay the time taken to respond to requests.</td></tr>
<tr><td colspan="2">Data Subject details whose records are requested (Please complete one form per person)</td></tr>
<tr><td>Surname:</td><td>Date of Birth:</td></tr>
<tr><td>Forename(s):</td><td rowspan="2">Current Address:

Full Postcode:</td></tr>
<tr><td>Any former names (if applicable):</td></tr>
<tr><td>Telephone Number:</td><td>Previous Address (if applicable):

Full Postcode:</td></tr>
<tr><td colspan="2">If further details are available please include in a separate covering note.</td></tr>
</table>

<table>
<tr><td colspan="2">Details of Information to be accessed
In order to locate the recordings that you require please provide as much information as possible.</td></tr>
<tr><td colspan="2">Date of incident: Time of incident:

Location of incident:</td></tr>
<tr><td>Please give a brief description of the incident including a description of yourself and clothing or any vehicle details (registration/model) if applicable, in order to help us identify you from the CCTV recordings.</td><td></td></tr>
</table>

Details of the Applicant (Complete if different to data subject details)	
Full Name	
Company (if applicable)	
Relationship with data subject	
Address to which a reply should be sent	**Postcode:** **Tel:**
Authorisation to release to applicant (to be completed by data subject if not making their own request)	

I (print name) _____

hereby authorise Warrington Borough Council to release personal data, as identified in the details of information to be accessed section, that they may hold relating to me to the above applicant and to whom I authorise to act on my behalf.

Signature of data subject:_____ Date:_____

Declaration
I declare that information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the information/record(s) referred to overleaf, under the terms of the Data Protection Act 2018
Please select one box below.

- ❑ I am the data subject.
- ❑ I have been asked to act on behalf of the data subject and they have completed the authorisation section above.
- ❑ I am acting on behalf of the data subject who is unable to complete the authorisation section above (Provide a covering letter with further details).
- ❑ I am the parent/guardian of a data subject under 16 years old who has completed the authorisation section above.
- ❑ I am the parent/guardian of a data subject under 16 years old who is unable to understand the request (Proof of parental responsibility may be required).
- ❑ I have been appointed the Guardian for the data subject, who is over age 16 under a Guardianship order (please attach).
- ❑ I am the deceased data subject's personal representative and attach confirmation of my appointment.
- ❑ I have a claim arising from the data subject's death and wish to access information relevant to my claim (Provide a covering letter with further details).

Print Name ……..

Signed (Applicant) …… **Date …**……..

Please Note:

- **You may be required to provide evidence of identity (i.e. copy of Driving Licence/Passport) and proof of address (e.g. copy of Council Tax, Utility Bill, Bank Statement)**
- **If there is any doubt about the applicant's identity or entitlement, information will not be released until further evidence is provided. You will be informed if this is the case.**
- **Access to CCTV footage can be denied if the footage is part of an ongoing police investigation and releasing this footage could prejudice the investigation.**
- **If identifiable images of other individuals occur as part of the requested data, access could be denied unless such parties consented or it is considered reasonable to comply with the request.**
- **Your information may be shared with other departments of the Council in order to fulfil your subject access request**

Please complete and send this document to:
Warrington Borough Council, Subject Access Requests, East Annexe, Town Hall, Sankey Street, Warrington WA1 1UH

Email: contact@warrington.gov.uk with 'Subject Access Request' in the subject line of the email.

Appendix F Regulation of Investigatory Powers Act Guiding Principles

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

The Regulation of Investigatory Powers Act 2000, amongst other subjects, relates to surveillance by the Police and other agencies (including Local Authorities) 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. Although The Systems cameras are overt if they are used in such a way that falls within the definition of Directed Surveillance they will only be used if the necessary verbal and/or written authorities have been given.

THE WARRINGTON CCTV SYSTEM CAMERAS WILL NOT BE USED FOR PURPOSES THAT MEET THE DEFINITION OF "INTRUSIVE SURVEILLANCE" UNLESS CORRECTLY AUTHORISED.

The impact for staff in the Police control rooms and CCTV monitoring centres, is that there might be cause to monitor for some time, a person or premises using the cameras.

In most cases, this will fall into sub section **c** above, i.e. it will be an immediate response to events or circumstances. In this case, it would not require authorisation.

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

In the case of authorities given by the Police these are usually authorised by a Superintendent or above. However, if an authority is required immediately, an Inspector may authorise the surveillance. The forms in both cases 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) for the purpose of preventing or detecting crime or of preventing disorder;

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

Written Authority must be granted, and the following details to be supplied to the CCTV Team Leader before using Warrington Borough Council CCTV for directed surveillance;

THE URN
THE DETAILS OF THE AUTHORISING OFFICER
COMMENCEMENT AND EXPIRY DATES
THE AUTHORISING OFFICERS STATEMENT OF WHAT HAS BEEN GRANTED (I.E COVERT USE OF LOCAL AUTHORITY CCTV)

The RIP Act also makes provision for directed surveillance to be conducted by a Local Authority. In such cases, the written authority to carry out directed surveillance using the Warrington CCTV System will only be given at Director or Head of Service level.