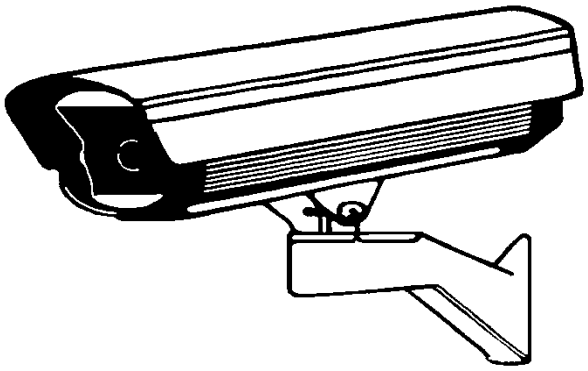
Leicester City Council

Leicester City Council

in partnership with

Leicestershire Police

CODE OF PRACTICE



for the Operation of

Leicester City Council

Closed Circuit Television Systems

City Centre Security

Version 1		Prior 2015
2		October 2015
3		October 2016
4		February 2020

CODE OF PRACTICE AGREED BY:

Leicester City Council
Leicestershire Police

Certificate of Agreement

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

Signed for and on behalf of Leicester City Council

Signature: .....….....

Name: ……. Position held: ……

Dated the .....…….. day of 200

Signed for and on behalf of Leicestershire Constabulary Area Commander

Signature: .....….....

Name: ……. Position held: ……

Dated the .....…….... day of 200

Signed for and on behalf of Traffic Management Service

Signature: .....….....

Name: ……. Position held: ……

Dated the .....…….... day of 200

Section 1 Introduction and Objectives

1.1 Introduction

A Closed Circuit Television (CCTV) system has been introduced since 1996 to Leicester City Centre. This system, known as Leicester City CCTV system, comprises a number of cameras installed at strategic locations. The cameras are a combination of pan, tilt and zoom , static and rapid deployables and their images are presented and recorded in a Monitoring Room located in premises owned by Leicester City Council, in Leicester City. Secondary monitoring and control facilities are located at Enderby Forces Headquarters, occasionally Euston Street Police Station and City Council Emergency Management Unit at City Hall. There are currently no recording facilities at any location other than the City Centre CCTV monitoring room. Images supplied to a third party shall be governed by their own Code of Practice, which shall be no less stringent than this document, and shall be the responsibility of the third party.

Leicester City Centre CCTV System has evolved from the formation of a partnership between Leicestershire Constabulary and Traffic Management Service who have all certified on the previous form their acceptance of the requirements of this Code.

For the purposes of this document, the 'owner' and the 'manager' of The System is Leicester City Council.

For the purposes of data protection legislation, the 'data controller' is Leicester City Council.

Leicester City Centre Security CCTV system has been notified to the Information Commissioner.

Details of key personnel, their responsibilities and contact points are shown at Appendix A to this Code.

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 of 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 is necessary, proportionate and suitable tool for all the objectives of The System listed in 1.3.1.

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 Leicester City Centre Security CCTV System may be perceived to infringe on the privacy of individuals. The Partnership 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.

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

1.2.5 Leicester City Centre Security 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 Leicester City CCTV System as determined by Leicester City Council which form the lawful basis for the processing of data are:

- *Assist in providing a better environment*
- *To help reduce the fear of crime.*
- *To help deter crime.*
- *To help detect crime and provide evidential material for Regina court proceedings.*
- *To assist in the overall management of Leicester City Centre.*
- *To assist in developing the economic well being of Leicester City Centre and encourage greater use of the City Centre.*
- *To assist Leicester City Council in its enforcement and regulatory functions within the City and County*
- *To assist in Traffic Management Schemes within the remit of the Council Authority*
- *To collect data for the study of transport use in the City and County*
- *To assist in the management of city events such as football matches, concerts and demonstrations.*
- *To assist a single or multi-agency response to a civil contingency or emergency as outlined in the City Council's action plan and Government legislation, for the purpose civil protection.*

1.3.2 Within this broad outline, Leicester City Council, in partnership with Leicestershire Constabulary, will draw up and publish specific key objectives (which will be reviewed periodically) based on local concerns.

1.4 Procedural Manual

This Code of Practice will be supplemented by a separate 'Procedural Manual', which will offer instructions on all aspects of the everyday operation of The System. To ensure the purpose and principles (see Section 2) of the CCTV system are realised, the procedural manual will be based and will expand upon the contents of this Code of Practice

Section 2 Statement of Purpose and Principles

2.1 Purpose

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

2.1.1 The 'Purpose' of Leicester City CCTV System and the process adopted in determining the 'Reasons' for its implementation are as previously defined in order to achieve the objectives detailed within Section 1.

2.2 General Principles of Operation

2.2.1 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 'Directed' surveillance or any surveillance of crime 'hotspot' areas, as required by the Regulation of Investigatory Powers Act 2000 and Leicestershire Constabulary procedure.

2.2.3 The System will be operated in accordance with current data protection legislation (e.g. the General Data Protection Regulation 2016, the Data Protection Act 2018) at all times.

2.2.4 The system will be operated in accordance with the Protection of Freedoms Act 2012.

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

2.2.6 The System will be operated with due regard to the principle that everyone has the right for their private life, family life and their home to be respected.

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

2.2.8 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.

2.2.9 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 Leicester City Council.

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 that can be recorded by the cameras accessed by The System.

2.4.2 None of the cameras forming part of The System will be installed in a covert manner. Appropriate signs will identify the presence of all cameras.

2.5 Monitoring and Recording Facilities

2.5.1 The CCTV equipment has the capability of recording selected cameras simultaneously throughout every 24 hour period.

2.5.2 CCTV operators are able to record images from selected cameras in real-time, produce hard copies 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 Control room or any recorded material without an authorised member of staff being present.

2.6.2 Specially selected and trained operators shall staff the monitoring room. This is in accordance with the strategy contained within the procedural manual.

2.6.3 All operators shall receive training relevant to their role in the requirements of the Human Rights Act 1998, the General Data Protection Regulation 2016, the Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000, the Freedom of Information Act 2000 and the Code of Practice and General Procedures. Further training will be provided as and when necessary.

2.7 Processing and Handling of Recorded Material

2.7.1 All recorded material, whether recorded digitally, in analogue format or as a hard copy video print, will be processed and handled strictly in accordance with this Code of Practice and the Procedural Manual.

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 or the Procedural Manual

2.9.1 Any major changes to either the Code of Practice or the Procedural Manual, which 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 Leicester City Council may implement a minor change, which will not have such a significant impact, without further consultation.

Note

I. *The installation of a CCTV camera is considered to* ***be overt*** *unless it is installed in a manner whereby it's deliberately intended to be concealed from the view of any person likely to be within the field of that camera. In which case the appropriate authorisation from Leicestershire Constabulary will have been received.*

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

Section 3 Privacy and Data Protection

3.1 Public Concern

3.1.1 Whilst the majority of the public support the use of CCTV, those who do express concern do so mainly over matters pertaining to the processing of the information, (or data) i.e. what happens to the material that is obtained.

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

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

3.1.3 The storage and security of the data will be strictly in accordance with the requirements of the General Data Protection Regulation 2016 and the Data Protection Act 2018 and additional locally agreed procedures.

3.2 Data Protection Legislation

3.2.1 The operation of Leicester City CCTV System has been notified to the office of the Information Commissioner in accordance with the Data Protection Act 2018.

3.2.2 The 'data controller' for Leicester City CCTV System is Leicester City Council and the responsibility for the data will be devolved to the CCTV Manager, of Leicester City Council's CCTV Service.

3.2.3 All data will be processed in accordance with the principles of the General Data Protection Regulation 2016 (see appendix B) which, in summarised form, includes:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability.

3.3 Request for information (subject access) and other data subject rights

3.3.1 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 Leicester City Council's City Centre CCTV Manager.

3.3.2 Articles 12 -22 of the GDPR and Schedule 2 of the Data Protection Act 2018 (Rights of Data Subjects) shall be followed in respect of every request. Those Sections are reproduced as Appendix B to this code.

3.3.3 If the request cannot be complied with without identifying another individual, permission from all parties must be considered (in the context of the degree of privacy they could reasonably anticipate from being in that location at that time) in accordance with the requirements of the legislation.

3.3.4 Any person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located. The appropriate 'Subject Access' National standard is given in Appendix C and a 'Subject Access' request form is included in Appendix D.

3.4 Exemptions to the Provision of Information

In considering a request made under the provisions of Schedule 2 of the Data Protection Act 2018, reference may also be made to Schedule 2, Part 1, Section 2 of the Act which includes, but is not limited to, the following statement:

3.4.1 Personal data processed for any of the following purposes -

i) The prevention or detection of crime

ii) The apprehension or prosecution of offenders

are exempt from the subject access provisions in any case 'to the extent that the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection'.

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

3.5 Criminal Procedures and Investigations Act, 1996

The Criminal Procedures and Investigations Act, 1996 came into effect in April 1997 and introduced a statutory framework for the disclosure to defendants of material which the prosecution would not intend to use in the presentation of its own case, (known as unused material). An explanatory summary of the provisions of the Act is contained within the procedural manual, but disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on Leicester City Council by Schedule 2 of the Data Protection Act 2018 (data subject access).

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.

4.1.2 Cameras will not be used to look into private residential property. Where the equipment permits it, 'Privacy zones' will be programmed into the system as required in order to ensure that the cameras do not survey the interior of any private residential property. The operators will be specifically trained in privacy issues.

4.1.3 A member of the public wishing to register a complaint with regard to any aspect of the CCTV System may do so by contacting Leicester City Council's CCTV Manager. All complaints shall be dealt with in accordance with Leicester City Council's complaints procedure, a copy of which may be obtained from Leicester City Council's Customer Service Centre, 91 Granby Street Leicester.

4.1.4 Any performance issues identified will be considered under Leicester City Council's disciplinary procedures.

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

4.2 System Owner and System Manager

4.2.1 The CCTV Manager, being the nominated representative of Leicester City Council, will have unrestricted personal access to the CCTV monitoring room and will be responsible for receiving regular and frequent reports from the CCTV Staffing Contract Manager. He/she will have day-to-day responsibility for the system as a whole and will ensure that every complaint is acknowledged in writing within five working days which will include advice to the complainant of the enquiry procedure to be undertaken.

4.3 Public Information

4.3.1 Code of Practice

Leicester City Council shall publish a copy of this Code of Practice and a copy will be made available to anyone on request.

4.3.2 Signs

Signs will be placed in the locality of the cameras and at main entrance points to the relevant areas. The signs will indicate the presence of CCTV monitoring and clearly identify Leicester City Council as the owner of the CCTV system providing contact details.

Section 5 Assessment of the System and Code of Practice

5.1 Evaluation

5.1.1 The System will periodically be evaluated to establish whether the purposes of the system are being complied with and whether objectives are being achieved. The evaluation will comprise but not be limited to:

i) *An assessment of the impact upon crime: This assessment shall include not only the immediate area covered by the cameras but the wider city area, the Police Divisional and regional areas and national trends.*

ii) *An assessment of the incidents monitored by The System*

iii) *An assessment of the impact on city centre business*

iv) *An assessment of neighbouring areas without CCTV*

v) *The views and opinions of the public*

vi) *The operation of the Code of Practice*

vii) *Whether the purposes for which the system was established are still relevant*

viii) *Cost effectiveness*

ix) *The security of the system*

5.1.2 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

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

5.2.2 The CCTV Manager shall also be responsible for maintaining full historical 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

5.3.1 The Contract Manager will be responsible for regularly auditing the operation of the system and the compliance with this Code of Practice. Audits, which may take the form of irregular spot checks, will include examination of the monitoring room records, disc histories and the content of recorded material.

Section 6 Human Resources

6.1 Staffing of the Monitoring Room and those responsible for the operation of Leicester City Council's CCTV System

6.1.1 The CCTV Monitoring Room will be staffed in accordance with the procedural manual. Authorised personnel who will have been properly trained in its use and all monitoring room procedures will only operate equipment associated with The System.

6.1.2 Every person involved in the management and operation of the system will have access to both the Code of Practice and the Procedural Manual, will be required to sign a confirmation that they fully understand the obligations adherence to these documents places upon them and that any breach will be considered as a disciplinary offence. They will be fully conversant with the contents of both documents, which may be updated from time to time, and which he/she shall be expected to comply with as far as is reasonably practicable at all times.

6.1.3 Arrangement may be made for a police officer to be present in the monitoring room at certain times, subject to locally agreed protocols and the Regulation of Investigatory Powers Act 2000. Any such person must also be conversant with this Code of Practice and associated Procedural Manual.

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

6.2 Discipline

6.2.1 Every individual employed by Leicester City Council 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 Leicester City Council's 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 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 room and for enforcing the discipline rules. Non-compliance with this Code of Practice by any person will be considered a severe breach of discipline and dealt with accordingly including, if appropriate, the instigation of criminal proceedings.

6.3 Declaration of Confidentiality

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

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.

7.1.2 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.

7.1.3 Cameras will not be used to look into private residential property. 'Privacy zones' can be programmed into the system and will be done so (whenever practically possible), in order to ensure that the cameras do not survey the interior of any private residential property within range of the system.

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

7.1.5 As a minimum, all operators will be issued with their own Corporate standard login and initial personal password. Where appropriate, individuals are expected to change their password to something they can remember and that it is discrete to themselves. All operators are expected to log off after their shift. Under no circumstances should operators allow others to use their logon credentials

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 Monitoring

7.3.1 Secondary monitoring facilities are provided at Leicestershire Constabulary Police Stations and at the Leicester City Council Emergency Management Unit. Currently there are links with Enderby Force Headquarters and Euston Street Police Station.

7.3.2 Subject to permission being granted by the Primary Control Room operator, secondary control rooms may take control of the operation of the cameras. The use of secondary control and monitoring facilities will be administered and recorded in full accordance with this Code of Practice and the Procedural Manual and does not diminish in any way the obligations imposed on any of the persons involved to comply with all current legislative requirements.

7.4 Operation of the System by the Police

7.4.1 Under certain 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 Leicester City Council, or designated deputy of equal standing. See Appendix G concerning the guiding principles to the Regulation of Investigatory Powers Act.

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

7.4.3 In very extreme circumstances, a request may be made for the Police to take total control of The System in its entirety, including the staffing of the monitoring room and personal control of all associated equipment, to the exclusion of all representatives of Leicester City Council. Any such request should be made to the CCTV Manager who will consult personally with the most senior officer of Leicester City Council (or designated deputy of equal standing). A request for total exclusive control must be made in writing by a police officer not below the rank of Assistant Chief Constable or person of equal standing.

7.5 Maintenance of the system

7.5.1 To ensure compliance with the Information Commissioner's Code of Practice and that images recorded continue to be of appropriate evidential quality, the Leicester City Council's City Centre CCTV System shall be maintained in accordance with these requirements under a maintenance agreement.

7.5.2 The maintenance agreement will make provision for regular/periodic service checks on the equipment, which will include checks on the functioning of the equipment and any minor adjustments that need to be made to the equipment settings to maintain picture quality.

7.5.3 The maintenance will also include regular periodic overhaul of all the equipment and the replacement of equipment that has reached the end of its serviceable life.

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

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 Manager 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, Monitoring Room 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 will be prohibited except for lawful, proper and sufficient reasons and only then with the personal authority of the CCTV Manager. Any such visits will be conducted and recorded in accordance with the Procedural Manual. See Appendix F – Restricted Access Notice.

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 visitor's book and a declaration of confidentiality.

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. In the event of the monitoring room having to be evacuated for safety or security reasons, the provisions of the Procedural Manual will be complied with.

8.5.2 The monitoring room will at all times be secured by 'Magnetic-Locks' operated by the CCTV operator or other equally secure means.

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, or on videotape or by way of video copying, including video prints.

Note
For the purpose of the Code the format is referred to as videotapes or recording, but this is a generic term. It may refer to any recording, prints, reviews, working copies, retention, release and tape register of videotapes, recorded in real or 12 hour time, single or multiplex or digital recording.

9.1.2 Every video or 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. The 'chain of handling' must be maintained to the highest degree to maintain the integrity of the evidence.

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, video tape, digital tape, CD, 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 and the Procedural Manual from they 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 National standard for the 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 CCTV Manager who will ensure that the principles contained within Appendix C 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 C 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. Under such circumstances, full details will be recorded in accordance with the Procedural Manual.

Note

The Police and Criminal Evidence Act 1984 [PACE] would cover release to the media of recorded information, in whatever format, which may be part of a current investigation. Any such disclosure should only be made after due consideration of the likely impact on a criminal trial. Full details of any media coverage must be recorded and brought to the attention of both the prosecutor and the defence.

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 and the Procedural Manual.

9.2.5 It may be beneficial to make use of 'real' video footage for the training and education of those involved in the operation and management of CCTV systems, and for those involved in the investigation, prevention and detection of crime. Any material recorded by virtue of this CCTV system will only be used for such bona fide training and education purposes. Recorded material will not be released for commercial or entertainment purposes. As per clause 2.3, the copyright will remain with Leicester City Council.

9.3 Digital Media and Video Tapes - Provision & Quality

9.3.1 Evidence is burned to a DVD via the CCTV system. Video tapes are no longer used.

9.4 DVD – Retention

9.4.1 CCTV recordings are held by the system for 28 days after which time the data is automatically overwritten. Downloaded, burned DVDs. are not retained. Before destruction, each DVD will be physically scored to prevent playback and tested in the system.

9.4.2 DVDs will be always be used and stored in accordance with the Procedural Manual.

9.5 DVD Register

9.5.1 Each DVD will have a unique tracking record maintained in accordance with the procedural manual,. The tracking record shall identify every use, and person who has viewed or took possession of the DVD.

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 either at 12.5 Images per second or where viewed on a spot monitor they will be recorded at 25 Images per second.

9.7 Evidential DVDs

9.7.1 The DVD is the evidential media.

9.8 CD / DVD Discs

9.8.1 Suitable quality CD / DVD discs will be used as per the quality declarations and findings of the Leicestershire Constabulary Forensic Team market survey 'Blank Media Analytical Report'. Wherever possible the Constabulary will provide discs in bulk for their use.

9.8.2 Video evidence will be burned to DVD / CD 's on request, the data release form will be signed by the investigating officer and the discs handed over. No evidence will be kept on the system after 28 days. The evidence burned to discs is in native format and can only be read by proprietary reader, which is automatically burned to the disc. The handed over evidence is the primary evidence.

a

Section 10 Video Prints

10.1 Guiding Principles

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

10.1.2 Video 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 in accordance with the Procedural Manual.

10.1.3 Video prints contain data and will therefore only be released under the terms of Appendix C to this Code of Practice, 'Release of data to third parties'. If prints are released to the media, (in compliance with Appendix C), in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with the Procedural Manual.

10.1.4 A record will be maintained of all video print productions in accordance with the Procedural Manual. 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, (if relevant) and the purpose for which the print was taken.

Appendix A Key Personnel and Responsibilities

1. System Owners

Leicester City Council
Local Services & Enforcement
City Hall
Charles Street
Leicester LE1 1FZ

Responsibilities:
Leicester City Council is the 'owner' of the system. The CCTV Manager will be the point of reference on behalf of the owner. His/her role will include a responsibility to:

i) Ensure the provision and maintenance of all equipment forming part of Leicester City Council City CCTV System in accordance with contractual arrangements, which Leicester City Council may from time to time enter into.

ii) Maintain close liaison with the control room supervisor.

iii) Ensure the interests of Leicester City Council and other organisations are upheld in accordance with the terms of this Code of Practice.

iv) Agree to any proposed alterations and additions to the system, this Code of Practice and/or the Procedural Manual.

v) Ensure that all users of the CCTV System are trained to the required standard in accordance with the terms of this Code of Practice.

The CCTV Manager has delegated authority for data control of Leicester City Council's City Centre Security CCTV System on behalf of Leicester City Council. Her/his role includes responsibility to:

1) Manage and supervise the CCTV system on behalf of the local authority and other members of the CCTV partnership.

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

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

4) Maintain direct liaison with operating partners.

5) Liase with the Police and other agencies as required.

6) Receive and decide upon all requests from other parties to view the System.

7) Ensure the effective training and supervision of CCTV operators.

8) Ensure the adequacy of procedures for the transfer of discs which are used in evidence to other parties, in particular to ensure those procedures preserve the continuity of evidence.

Advise on the operational use of the System.

2. System Management

CCTV Manager

Traffic Management - Maintenance and Support

Leicester City Council
Traffic Management Service
York House
91 Granby Street
Leicester
LE1 6FB

Appendix B
Extracts from the GDPR and Data Protection Act 2018

GDPR Article 12

1. [1]The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. [2]The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. [3]When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. [1]The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. [2]In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. [1]The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. [2]That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. [3]The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. [4]Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. [1]Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. [2]Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

    1. charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

    2. refuse to act on the request.

    [3]The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

GDPR Article 15

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

    I. the purposes of the processing;
    II. the categories of personal data concerned;
    III. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

IV. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
V. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
VI. the right to lodge a complaint with a supervisory authority;
VII. where the personal data are not collected from the data subject, any available information as to their source;
VIII. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. [1]The controller shall provide a copy of the personal data undergoing processing. [2]For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. [3]Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

GDPR Article 17

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

    1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

    2. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

    3. the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

    4. the personal data have been unlawfully processed;

    5. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

    6. the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

    1. for exercising the right of freedom of expression and information;

    2. for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

3. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

4. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

5. for the establishment, exercise or defence of legal claims.

GDPR Article 18

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

    1. the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

    2. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

    3. the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

    4. the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

GDPR Article 21

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. [2]The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have

the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

GDPR Article 22

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

    1. is necessary for entering into, or performance of, a contract between the data subject and a data controller;

    2. is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

    3. is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

DATA PROTECTION PRINCIPLES

THE FIRST DATA PROTECTION PRINCIPLE

This requires that personal data shall be processed fairly and lawfully, and, in particular, shall not be processed unless:
a) at least one of the conditions in Article 6 is met, and
b) in the case of special category personal data, at least one of the conditions in Article 9 is also met".

To assess compliance with this Principle, it is recommended that the data controller address the following questions:

A. Are personal data and/or sensitive personal data processed?

The definition of special category (sensitive) personal data has been discussed and it is essential that the data controller has determined whether they are processing information/images. This is in order to access which criteria to consider when deciding whether there is a legitimate basis for the processing of that information / image.

B. Has a condition for processing been met?

The first data protection principle requires that the data controller have a legitimate basis for processing. It is for the data controller to be clear about which grounds to rely on in this respect. These are set out in Articles 6 and 9 of the GDPR and Schedule 1 of the Data Protection Act 2018.

Users of schemes which monitor spaces to which the public have access, such as town centres, may be able to rely on GDPR Article 6 1(e) because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller This could include purposes such as prevention and detection of crime, apprehension and prosecution of offenders or public/employee safety.

It should be noted that while this criterion may provide a general ground for processing, in an individual case, the interests of the data controller i.e. the user of the surveillance equipment might not outweigh the rights of an individual.

If the data controller has determined that he or she is processing sensitive personal data, then the data controller will also need to determine whether they have a legitimate basis for doing so under GDPR Article 9 and/ or Schedule 1 of the Data Protection Act 2018.

c) Are the information/images processed lawfully?

The fact that the data controller has a lawful basis for processing does not mean that this element of the first data protection principle is automatically satisfied.

The data controller will also need to consider whether the information /images processed are subject to any other legal duties or responsibilities such as the common law duty of confidentiality. Public sector bodies will need to consider their legal powers under administrative law in order to determine whether there are restrictions or prohibitions on their ability to process such data. They will also need to consider the implications of the Human Rights Act 1998.

d) Are the information/images processed fairly?

The fact that a data controller has a legitimate basis for processing information/images will not automatically mean that this element of the first data protection principle is satisfied.

The interpretive provisions of the GDPR set out what is required in order to process fairly. In order to process fairly, the following information, at least, must be provided to the individuals at the point of obtaining their images:

- the identity of the data controller
- the identity of a representative the data controller has nominated for the purposes of the General Data Protection Regulation 2016
- the purpose or purposes for which the data are intended to be processed, and
- any information which is necessary, having regard to the specific circumstances in which the data are or are to be processes, to enable processing in respect of the individual to be fair.

e) Circumstances in which the requirement for signs may be set aside

The General Data Protection Regulation 2016 and Data Protection Act 2018 does not make specific reference to the use of covert processing of special category (sensitive) personal data but it does provide a limited exemption from the requirement of fair processing. Because fair processing (as indicated above) requires that individuals are made aware that they are entering an area where their images may be captured, by the use of signs, it follows that the use of covert processing i.e. removal or failure to provide signs, is prima facie a breach of fairness of the first data protection principle. However, a breach of this requirement will not arise if an exemption can be relied on. Such an exemption may be found at Schedule 2, part 1, Section 2 of the Data Protection Act 2018, which states that:

"Personal data processes for any of the following purposes:

a) prevention or detection of crime
b) apprehension or prosecution of offenders

are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Articles 6 & 9) to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned."

In effect this means that the data controller can process images for either or both of the purposes listed in the exemption, may be able to obtain and process images without signs without breaching the fairness requirements of the first data protection principle.

THE SECOND DATA PROTECTION PRINCIPLE

This requires that

"Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes."

In order to ascertain whether the data controller can comply with this data protection principle it is essential that he / she is clear about the purpose(s) for which the images are processed.

Specified purposes may be those, which have been notified to the Commissioner or to the individuals.

There are a number of issues to be considered when determining lawfulness:

- Whether the data controller has a legitimate basis for the processing (see fist principle)
- Whether the images are processed in accordance with any other legal duties to which the data controller may be subject e.g. the common law duty of confidence, administrative law etc

It is quite clear from the interpretive provisions to the principle that the requirement of compatibility is particularly significant when considering making a disclosure to a third party or developing a policy on disclosures to third parties. If the data controller intends to make a disclosure to a third party, regard must be had to the purpose(s) for which the third party may process the data.

This means, for example, that if the purpose(s) for which images are processed is:

- Prevention or detection of crime
- Apprehension or prosecution of offenders

The data controller may only disclose to third parties who intend processing the data for compatible purposes. Thus, for example, where there is an investigation into criminal activity, disclosure of footage relating to that criminal activity to the media in order to seek assistance from the public in identifying the perpetrator, the victim or witnesses, may be appropriate. However, it would be an incompatible use if images from equipment installed to prevent or detect crime were disclosed to the media merely for entertainment purposes.

If it is determined that a particular disclosure is compatible with the purposes for which the data controller processes images, then the extent of disclosure will need to be considered. If the footage, which is to be disclosed, contains images of unrelated third parties, the data controller will need to ensure that those images are disguised in such a way that they cannot be identified.

If the data controller does not have the facilities to carry out such editing, he or she may agree with the media organisation that it will ensure that those images are disguised. This will mean that the media organisation is carrying out processing, albeit of a limited nature on behalf of the data controller which is likely to render it a data processor. In which case the data controller will need to ensure that the relationship with the media

organisation complies with the seventh data protection principle.

THE THIRD DATA PROTECTION PRINCIPLE

This requires that:

"Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed".

This means that consideration must be given to the situation of the cameras so that they do not record more information than is necessary for the purposes for which they were installed. For example cameras installed for the purpose of recording acts of vandalism in a car park should not overlook private residences. Futhermore, if the recorded images on the tapes are blurred or indistinct, it may well be that this will constitute inadequate data. For example, if the purpose of the system is to collect evidence of criminal activity, blurred or indistinct images from degraded tapes or poorly maintained equipment will not provide legally sound evidence and may therefore be inadequate for its purpose.

THE FOURTH DATA PROTECTION PRINCIPLE

This requires that:

"Personal data shall be accurate and where necessary, kept up to date."

This principle requires that the personal information that is recorded and stored must be accurate. This is particularly important if the personal information taken from the system is to be used as evidence in cases of criminal conduct or in disciplinary disputes with employees. The Commissioner recommends that efforts are made to ensure the clarity of the images, such as using only good quality tapes in recording information, cleaning the tapes prior to re-use and not simply recording over existing images and replacing tapes on a regular basis to avoid degradation from over-use.

If the data controller's system uses features such as time references and even location references, then these should be accurate. This means having a documented procedure to ensure the accuracy of such features are checked and if necessary, amended or altered.

Care should be exercised when using digital enhancement and compression technologies to produce stills for evidence from tapes because these technologies often contain pre-programmed presumptions as to the likely nature of sections of the image. Thus the user cannot be certain that the images taken from the tape are an accurate representation of the actual scene. This may create evidential difficulties if they are to be relied on either in court or an internal employee disciplinary hearing.

THE FIFTH DATA PROTECTION PRINCIPLE

This requires that

"Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes."

This principle requires that the information shall not be held for longer than is necessary for the purpose for which it is to be used. Normally, digital recordings will be retained on the system for 28 days from date origination after which they are automatically erased. The digital recordings or tapes that have recordings of relevant activities will be made available to authorised bodies. In the case of digital discs, no primary evidence

will be retained by the system after 28 days. In the case of video tapes, were they are used, these should be retained until proceedings are completed and the possibility of any appeal has been exhausted. After that time, the tapes should be erased. Apart from those circumstances, stored or recorded images should not be kept for any undue length of time. A policy on periods for retention of the images should be developed which takes into account the nature of the information and the purpose for which it is being collected. For example where images are being recorded for the purposes of crime prevention in a shopping area, it may be that the only images that need to be retained are those relating to specific incidents of criminal activity; the rest could be erased after a very short period. The commissioner understands that generally town centre schemes do not retain recorded images for more than 28 days unless the images are required for evidential purposes.

THE SIXTH DATA PROTECTION PRINCIPLE

This requires that

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

In order to access the level of security the data controller needs to take to ensure compliance with this Principle, he or she needs to access:

- The harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage of the personal data. While it is clear that breach of this principle may have a detrimental effect on the purpose(s) of the scheme e.g. the evidence or images might not stand up in court, or the public may lose confidence in your use of surveillance equipment due to inappropriate disclosure, the harm test requited also requires primarily the effect on the people recorded to be taken into account;
- The nature of the data to be protected must be considered. Special category (sensitive) personal data was defined at the beginning of this part of the code, but there may be other aspects, which need to be considered. For example, a town centre scheme may coincidently record the image of a couple kissing in a parked car, or a retailer's scheme may record images of people in changing rooms (in order to prevent items of clothing being stolen). Whilst these images may not fall within the sensitive categories as set in section 2, it is clear that the people whose images have been captured will consider that information or personal data should be processed with greater care.

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

(1) Introduction

Arguably CCTV is a powerful tool to be developed during recent years to assist with efforts to combat crime and disorder whilst enhancing community safety. Equally, some regard CCTV 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.

Leicester City Council and their partners 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 tool, for civic security and as well as a myriad of other uses, those people who do express concern tend to do so over the handling of the information (data) that the System gathers.

Leicester City Council has adopted the following nationally recommended standard.

(2) General Policy

All requests for the release of data shall be processed in accordance with the Procedure Manual. All such requests shall be channelled through Leicester City Council.

(3) Primary Request To View Data

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

- i) Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996, etc.);
- ii) Providing evidence in civil proceedings or tribunals
- iii) The prevention of crime
- iv) The investigation and detection of crime (may include identification of offenders)
- v) Identification of witnesses

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

- i) Police
- ii) Statutory authorities with powers to prosecute, (e.g. Customs and Excise; Trading Standards, etc.)
- iii) Solicitors
- iv) Plaintiffs in civil proceedings
- v) Accused persons or defendants in criminal proceedings
- iii) Other agencies, (which should be specified in the Code of Practice) according to purpose and legal status).

c) Upon receipt from a third party of a bona fide request for the release of data, Leicester City Council 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), Leicester City Council, or nominated representative, shall:

i) Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.

ii) Treat all such enquiries with strict confidentiality.

Notes

(1) The release of data to the police is not 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) Leicester City Council 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) Leicester City Council 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)

(4) Secondary Request To View Data

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

i) The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. General Data Protection Regulation 2016, Data Protection Act 2018, 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 General Data Protection Regulation 2016 and the Data Protection Act 2018);

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

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.

(5) Individual Subject Access under Data Protection legislation

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

I. Leicester City Council is supplied with sufficient information to satisfy him or her self as to the identity of the person making the request;

II. The person making the request provides sufficient and accurate information about the time, date and place to enable Leicester City Council 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);

III. 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 Leicester City Council 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) Leicester City Council 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) Leicester City Council is also entitled to refuse the request if it is considered to be manifestly unfounded or excessive.

e) In addition to the principles contained within the Data Protection legislation, Leicester City Council 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;

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

6. Process of Disclosure:

a) Verify the accuracy of the request.

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

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

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

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

7. Media disclosure

Set procedures for release of data to a third party should be followed. If the means of editing out other personal data does not exist on-site, measures should include the employment of professional services to act on behalf of the system owners.

a) 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 Leicester City Council, e.g. specific identities/data that must not be revealed.

iii) It shall require that proof of any editing must be passed back to Leicester City Council, 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.

8. 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;

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

Appendix D Subject Access Request Form

LEICESTER CITY COUNCIL CCTV SURVEILLANCE SYSTEM
General Data Protection Regulation 2016 / Data Protection Act 2018

How to Apply For Access To Information Held On the CCTV System

These notes explain how you can find out what information, if any, is held about you on the CCTV System.

Your Rights

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate, manifestly-unfounded effort, or if you agree otherwise. Leicester City Council will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, the Council is not obliged to comply with an access request unless –

- The other individual has consented to the disclosure of information, or
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual(s)

The Council's Rights

Leicester City Council may deny access to information where the data protection legislation allows. The main exemptions in relation to information held on the CCTV System are where the information may be held for:

- Prevention and detection of crime
- Apprehension and prosecution of offenders

And giving you the information may be likely to prejudice any of these purposes.

Fee

There is no fee unless a request is a repeat request.

THE APPLICATION FORM: **(N.B. ALL sections of the form must be completed. Failure to do so may delay your application.)**

Section 1 Asks you to give information about yourself that will help the Council to confirm your identity. The Council has a duty to ensure that information it holds is secure and it must be satisfied that you are who you say you are.

Section 2 Asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, date of birth and current address) together with a recent full-face photograph of you. A description of your appearance at the time of the incident will also help us to identify you in any footage.

Section 3 Asks you to confirm whether you will accept just viewing the information, or if you want a copy of the information.

Section 4 **You must sign the declaration**

When you have completed and checked this form, please send it together with the required TWO identification documents, with photograph and information about appearance to: Information Governance & Risk, City Hall, 115 Charles Street, Leicester, or email via info.requests@leicester.gov.uk

You can now also apply for CCTV footage via the Council's website at www.leicester.gov.uk

If you have any queries regarding this form, or your application, please contact Information Governance & Risk.

LEICESTER CITY COUNCIL CCTV SURVEILLANCE SYSTEM
General Data Protection Regulation 2016/ Data Protection Act 2018

SECTION 1 About Yourself

The information requested below is to help the Council (a) satisfy itself as to your identity and (b) find any data held about you.

PLEASE USE BLOCK LETTERS

Title *(tick box as appropriate)*	Mr		Mrs		Miss		Ms	
Other title *(e.g. Dr., Rev., etc.)*								
Surname/family name								
First names								
Sex *(tick box)*	Male				Female			
Height								
Date of Birth								
Place of Birth	Town							
	County							

Your Current Home Address *(to which we will reply)*	
	PostCode
A telephone number will be helpful in case you need to be contacted.	Tel. No.

If you have lived at the above address for less than 10 years, please give your previous addresses for the period:

Previous address(es)		
Dates of occupancy	From:	To:
Dates of occupancy	From:	To:

SECTION 2 Proof of Identity

To help establish your identity your application must be accompanied by **TWO** official documents that between them clearly show your name, date of birth and current address.

For example: a birth/adoption certificate, driving licence, medical card, passport or other official document that shows your name and address.

Also a recent, full face photograph of yourself and a description of your appearance at the time of the incident in question.

Failure to provide this proof of identity may delay your application.

SECTION 3 Supply of Information

You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to:

(a) View the information and receive a permanent copy YES / NO

(b) Only view the information YES / NO

SECTION 4 Declaration

DECLARATION (to be signed by the applicant)

The information that I have supplied in this application is correct and I am the person to whom it relates.

Signed by Date

Warning – a person who impersonates or attempts to impersonate another may be guilty of an offence.

NOW – please complete Section 4 and then check the 'CHECK' box (on page 5) **before returning the form.**

SECTION 5 To Help us Find the Information

If the information you have requested refers to a specific offence or incident, please complete this Section.

Please complete a separate box in respect of different categories/incidents/involvement. Continue on a separate sheet, in the same way, if necessary.

If the information you require relates to a vehicle, property, or other type of information, please complete the relevant section overleaf.

Were you: (tick box below)

A person reporting an offence or incident	
A witness to an offence or incident	
A victim of an offence	
A person accused or convicted of an offence	

Other – please explain	

Date(s) and time(s) of incident	
Place incident happened	
Brief details of incident	

LEICESTER CITY COUNCIL CCTV SURVEILLANCE SYSTEM
General Data Protection Regulation 2016 / Data Protection Act 2018

Before returning this form	• Have you completed ALL Sections in this form?
Please check:	• Have you enclosed TWO identification documents?
	• Have you signed and dated the form?

Further Information:

These notes are only for guidance. The law is set out in the General Data Protection Regulation and the Data Protection Act 2018. Further information and advice may be obtained from:

The Office of the Information Commissioner (ICO),
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF.
Tel. (01625) 545745
www.ico.org.uk

Please note that this application for access to information must be made direct to **Leicester City Council** (address on Page 1) and **NOT** to the ICO.

OFFICIAL USE ONLY

Please complete ALL of this Section (refer to 'CHECK' box above).

Application checked and legible? ☐

Identification documents checked? ☐

Details of 2 Documents (see page 3)

Date Application Received

Fee Paid

Method of Payment

Receipt No.

Documents Returned?

Member of Staff completing this Section:

Name

Location

Signature

Date

Appendix E Declaration of Confidentiality

Leicester City Centre CCTV System

I, ……..., am retained by (Contractor's name). On behalf of Leicester City Council to perform the duty of CCTV Control Room Operator. I have received a copy of the Code of Practice in respect of the operation and management of that CCTV System.

I hereby declare that:

I am fully conversant with the content of that Code of Practice and understand that all duties which I undertake in connection with Leicester City Council's City Centre Security 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 (contractor's name) 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 F Restricted Access Notice

WARNING

RESTRICTED ACCESS AREA

All visitors MUST sign in the log book

Be advised entry to the Control Room is conditional on acceptance of the following confidentiality clause:

ALL persons entering the CCTV control rooms must sign in via this access log, in doing so you agree not to divulge the location of the control room, personal details of the operators or any information obtained, overheard or seen during the visit. All such information is covered by the General Data Protection Regulation 2016 and Data Protection Act 2018 and may render you open to prosecution.

The use of Mobile Phones (except for work purposes) is strictly prohibited

The use of Body Worn Video or any other device to record images is strictly prohibited

CCTV IMAGES ARE BEING RECORDED WITHIN THIS CONTROL ROOM

Appendix G Regulation of Investigatory Powers Act Guiding Principles

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

The Regulation of Investigatory Powers Act 2000 relates to surveillance by the Police and other agencies and deals in part with the use of directed, covert and intrusive 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

CCTV being used intrusively will be authorised other than by this section of the Act. Appropriate guidelines already exist for intrusive surveillance.

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 unless it were to continue for some time. The code says some hours rather than minutes.

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.

Slow time requests are authorised by a Superintendent or above.

If an authority is required immediately, an Inspector may do so. 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) in the interests of national security;

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

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

(d) in the interests of public safety;

(e) for the purpose of protecting public health;

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

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

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

Forms should be available at each CCTV monitoring centre and are included in the procedural manual and available from the CCTV User Group Website

Examples:

Insp. Authorisation
An example of a request requiring Inspector authorisation might be where a car is found in a car park late at night and known to belong to drug dealers. The officers might task CCTV to watch the vehicle over a period of time to note who goes to and from the vehicle.

Supt Authorisation
Where crime squad officers wish to have a shop premises monitored from the outside, which is suspected of dealing in stolen goods over a period of days.

No Authorisation
Where officers come across a local drug dealer sitting in the town centre/street and wish to have the cameras monitor them, so as not to divulge the observation taking place.

Presentation of DSA
In all cases, where Police attend the CCTV Control room to carry out directed / Intrusive surveillance, the name of the DSA must be entered into the visitor's log book.

The operators will check to make sure that such an authorised RIPA is in possession of the City Council.

Where such a DSA is not in existence, the control room operator will refer the matter to the CCTV Manager.