CITY OF Lincoln COUNCIL

Code of Practice For the Operation of Closed Circuit Television

Issued

June 2026

Document control

Organisation	City of Lincoln Council
Title	Code of Practice for the Operation of Closed-Circuit Television
Author - name and title	JH/AW
Owner - name and title	Community Services Manager – Jonathan Hammond
Date	
Approvals	Policy Scrutiny 09/06/2026 Executive 14/07/2026
Filename	
Version	7
Next review date	June 2029

Document Amendment history

Revision	Originator of change	Date of change	Change description
November 2025	AW/JH		Update from Version 6 to Version 7

Distribution and training history

Details	Date

Contents

Certificate of Agreement		**4**
Section 1:	**Introduction and Objectives**	**5**
Section 2:	**Statement of Purpose and Principles**	**7**
Section 3:	**Privacy and Data Protection**	**10**
Section 4:	**Accountability and Public Information**	**13**
Section 5:	**Assessment of the System**	**14**
Section 6:	**Staff**	**15**
Section 7:	**Control By, and Communication with, Other Schemes, Partners and Organisations**	**17**
Section 8:	**Access to and Security of Control Room and Associated Equipment**	**18**
Section 9:	**Management of Recorded Material**	**19**

Appendices

A	**Key Personnel and Responsibilities**	**23**
B	**Extract from and Principles of Data Protection Legislation**	**24**
C	**National Standard for the Release of Data to Third Parties**	**25**
D	**Not used**	
E	**Control Room Warning-Confidentiality Notice**	**31**
F	**The 12 Guiding Principles of the Surveillance Camera Code of Practice**	**32**
G	**RIPA Guiding Principles**	**33**
H	**Glossary of terms**	**35**

CCTV System Code of Practice

Certificate of Agreement

The content of this Code of Practice is hereby approved in respect to the City of Lincoln Council 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 City of Lincoln Council

Signature:…….

Name: ……

Position held: ……

Date……..

Signed for and on behalf of Lincolnshire Police

Signature: ……

Name: ……

Position held: ……

Date……..

Section 1 Introduction and Objectives

1.1 Introduction

1.1.1 The City of Lincoln Council (Hereafter referred to as CoLC) Public Spaces CCTV system was set up in 1996. It is owned and operated by the City of Lincoln Council at City Hall, Beaumont Fee, Lincoln, LN1 1DD. Details of key personnel, their responsibilities and contact points are shown in appendix A to this Code of Practice, (hereafter referred to as 'the Code'). A public space for the purpose of this Code is described as 'A place to which the public have access whether on payment or not.'

1.1.2 All recorded material is owned by, and copyright of, the City of Lincoln Council. The CCTV system comprises of a number of cameras installed at strategic locations. The cameras are fully operational with pan, tilt and zoom PTZ) facilities and static cameras, Body Worn Cameras (BWC) and Re-Deployable Cameras (RDC). Data is primarily transmitted to the CCTV control room by wireless transmissions. The CCTV system is monitored from a strategic, purpose-built Control Room based at City Hall in Lincoln. For the purposes of the Data Protection Act the 'Data Controller' is the City of Lincoln Council.

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

1.1.3 It is recognised that operation of the CoLC CCTV system may be considered by some as an infringement on the privacy of individuals. CoLC recognises that it has a responsibility to ensure that the scheme always complies with all relevant legislation in order to ensure its legality and legitimacy. The scheme will only be used as a proportionate response and only as far as it is necessary in a democratic society, in the interests of national security, for public safety, for the economic well-being of the area, for the prevention and detection of crime or disorder, for the protection of public health and safety, and for the protection of rights and freedoms of others.

1.2 Key Legislation

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

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

1.2.3 Protection of Freedoms Act 2012 (PoFA 2012) including 12 Guiding Principles (See Appendix F). This Act provides for the destruction, retention, use and other regulation of certain evidential material. A code of practice is issued by the Secretary of state under sections 29-31 of PoFA 2012. It provides guidance on the appropriate and effective use of surveillance camera systems by relevant authorities (as defined by Section 33(5) of PoFA 2012) in England and Wales who must, under Section 33(1) of PoFA 2012, have regard to the code when exercising any functions to which the code relates. CoLC is a relevant authority for these purposes and therefore subject to the Secretary of state's code of practice. The code can be found here www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version.The Information Commissioner's Officer have also updated their Video Surveillance guidance which can be found here Video surveillance (including guidance for organisations using CCTV) | ICO

1.2.4 The Data Protection Legislation includes but is not limited to the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR) and the Data (Use and Access) Act 2025. Everyone responsible for using personal data must follow strict rules called 'data protection principles' (see 3.2.4). They must make sure the information is used fairly, lawfully and transparently.

1.2.5 Regulation of Investigatory Powers Act 2000 (RIPA) (See Appendix G) governs the use of covert surveillance by public bodies.

1.2.6 The Equality Act 2010 protects people from discrimination in the workplace and in wider society and makes it unlawful for someone to be discriminated against on the grounds of any of the protected characteristics set out in the Act: Age, Disability, Gender reassignment, Marriage and civil partnership, Pregnancy and maternity, Race, Religion and belief, Sex, Sexual orientation.

1.3 Aims of the CCTV System

1.3.1 The Aims of the scheme are:

a) To enhance community safety

b) To help secure a safer environment for those people who live in, work in and visit the areas

c) The detection, deterrence and prevention of crime such as:

Providing assistance in the prevention of crime.
Deterring and detecting crime.
Helping to identify, apprehend and prosecute offenders.
Providing the Police with evidence to take criminal action in the courts.

d) To assist in aspects of traffic management

e) To assist in the delivery of City Council services such as quick identification of damaged street furniture to be mended or replaced, street cleansing issues including identification of fly tipping for removal and highlighting Health and Safety matters

f) To reduce the fear of crime and to provide reassurance to the public

g) To assist in the improvement of the environment and the security of the areas, to make the city a more attractive and safe area to live, shop, work or socialise in, throughout the day and night time 'Safer Streets' economy.

h) To help with the communication and operational response of Police patrols in and around the city

i) To assist in the finding of missing people and assist when searching for vulnerable people and high-risk individuals threatening suicide.

1.4 Operations Procedures Manual

1.4.1 The Code is supplemented by a separate 'Operations Procedures Manual' providing instructions on all aspects of the day-to-day operation of the system. To ensure that the purpose and principles (see Section 2) of the CCTV system are realised, the Operations Procedures Manual is based upon and expands on the contents of the Code.

Section 2 Statement of Purpose and Principles

2.1 General Purpose and Principles of Operation

2.1.1 The purpose of this document is to state the intention of the CoLC and its staff to support the Aims of the CoLC CCTV system, (hereafter referred to as 'the system') and to outline how it will do this.

2.1.2 The system will be operated in accordance with all the requirements and the principles of current legislation, the Amended Surveillance Camera Code of Practice (accessible version) - GOV.UK (www.gov.uk), this Code and CoLC policies and procedures.

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

2.1.4 The system will be operated with due regard to the principle that everyone has the right to respect for their private and family life.

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

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

2.1.7 Throughout the Code it is intended, as far as reasonably possible, to balance the Aims of the system with the need to safeguard individual's rights. The Code shows that a formal structure has been put in place, including a complaints procedure, by which the system is not only accountable but is seen to be accountable.

2.1.8 Participation in the system by any organisation, individual or authority assumes an agreement by all such participants to comply with the Code. The Code will be provided to all new participants prior to their involvement with the service.

2.2 Cameras and Area Coverage

2.2.1 The Areas covered by CoLC CCTV to which the Code refers include:

Lincoln City Centre - Uphill and Downhill, Transport Hub, St Marks Shopping Centre, some public parks, residential areas on the edge of the city centre (Park ward, Abbey ward, Carholme ward and Castle ward), some city centre car parks, some council offices (public areas) and Housing properties, Yarborough Leisure Centre, Birchwood Leisure Centre, Community Centres, CoLC Managed Workspaces, Bracebridge Heath recreation field and Forum Centre North Hykeham.

These are hereafter referred to as 'the Area.'

2.2.2 The system is a mix of pan tilt and zoom (PTZ) cameras and static cameras. All have full colour capability; some of the cameras have infra-red and monochrome options. Body Worn Cameras (BWC) and Re-deployable Cameras (RDC) are also included in the system and are covered by the Code.

2.2.3 No dummy cameras will be used in the system. It is important not to make false claims about the effectiveness of the system, to avoid raising false expectations. Public confidence afforded by the system should be based on

effective operating cameras and dummy cameras have no place in such a system.

2.2.4 DPIAs (Data Protection Impact Assessments) are in place for all existing cameras, and these are reviewed annually. Any expansion of the system will be tested by a DPIA and will be in line with current legislation and the Code.

2.2.5 The system includes cameras on land belonging to other organisations, in which case a charge is made for maintenance and monitoring, with reference to the Charging Policy. Some internal charges, within CoLC, are made with reference to land ownership.

2.3 Monitoring and Recording Facilities

2.3.1 The Control Room is located at City Hall, Lincoln. The CCTV equipment has the capability of recording all cameras connected to the Control Room simultaneously and continuously.

2.3.2 No equipment, other than that which is housed within the main CCTV control room, and other specified council buildings where appropriate, shall be capable of recording images from any of the cameras.

2.3.3 CCTV Operators can upload relevant footage to internal recipients (CoLC Responsible Managers) on request through One Drive subject to authorisation from the CCTV Team Leader or Community Services Manager.

2.3.4 The CCTV Control Room shall be staffed by trained operators and operate in accordance with CoLC policy and procedures.

2.3.5 All operators shall be licensed by the Security Industry Authority (the SIA) and receive training relevant to their role in the requirements of the Human Rights Act 1998, Data Protection Legislation, Regulation of Investigatory Powers Act 2000 and the Codes of Practice and Procedures. Training will be provided as necessary.

2.3.6 None of the cameras forming part of the system will be installed in a covert manner. The presence of CCTV cameras will be identified by appropriate signs. In exceptional circumstances, and under a RIPA process, it may be necessary to install a camera or cameras covertly as part of a specific operation, for the duration of that operation.

2.4 Operators Instructions

2.4.1 Technical instructions on the use of equipment housed within the Control Room are contained in separate manuals provided by the equipment suppliers.

2.4.2 The Operations Procedures Manual sets out how operations will ensure compliance with this Code.

2.5 Changes to the Code

2.5.1 Any major changes to the Code (i.e., those that will have a significant impact upon the Code or upon the operation of the system) will take place only after all organisations with a participatory role in the operation of the system have been notified.

2.5.2 A minor change (i.e., one which may be required for clarification and will not have such a significant impact) will be agreed by the Portfolio Holder.

2.5.3 All major changes will be approved by the Council's Executive Committee.

2.5.4 A formal review of the Code will take place every three years and will be approved by the Council's Executive, or in the event there are no significant changes, the relevant Portfolio Holder.

Section 3 Privacy and Data Protection

See also Appendix B.

3.1 Data Collection

3.1.1 All personal data obtained by virtue of the system, shall be processed fairly, lawfully and in a transparent manner and shall only be processed in the exercise of achieving the stated objectives of the system.

3.1.2 The collection, processing, storage and security of the data will be strictly in accordance with the requirements of the Data Protection Legislation.

3.2 Data Protection Legislation

3.2.1 The operation of the system has been notified to the Office of the Information Commissioner in accordance with current Data Protection Legislation. Information Commissioner's Office

3.2.2. The data controller for the system is CoLC and day to day responsibility for the data will be devolved to the CCTV Team Leader.

3.2.3 DPIAs will be reviewed as part of an ongoing monitoring process taking into account changes to the system area. DPIAs will be reviewed annually. A DPIA will be undertaken for each addition to the system prior to any installation taking place.

3.2.4 All data will be processed in accordance with the principles of the Data Protection Legislation, which states in Article 5 of UK GDPR that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency').

(b) collected whether from the data subject or otherwise for specified, explicit and legitimate purposes and not further processed by or on behalf of a controller in a manner that is incompatible with the purposes for which the controller collected the data ('purpose limitation').

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

(g) The controller shall be responsible for, and be able to demonstrate compliance with, these principles ('accountability')."

3.2.5 —Individuals can ask to access their personal data and/or to be informed of certain information regarding how their personal data is being processed, and CoLC has a process for this which starts with the completion, by the requester, of an online form- Make a subject access request – City of Lincoln Council. Data will not be released under this process if other third parties can be identified in the footage.

3.3 Regulation of Investigatory Powers Act 2000 (RIPA)

3.3.1 RIPA 2000 came into force in October 2000 to regulate the use of relevant investigatory powers in accordance with human rights. The Act has been significantly updated and amended since. The Act regulates both 'Directed' and 'Intrusive' surveillance.

3.3.2 With regard to “Directed” surveillance, S.26 (2) of the Act, defines this as a pre-planned activity, which is

‘Covert surveillance that is undertaken in relation to a specific investigation or a specific operation which is likely to result in obtaining private information about a person.’

3.3.3 On occasions the CCTV system may be used to undertake “Directed” surveillance providing the purpose of such surveillance is compatible with the provisions contained within the Act including any amendments as defined in the Protection of Freedoms Act 2012. It is anticipated that the majority of such surveillance will be:

a) For the purpose of preventing or detecting crime or preventing disorder
b) In the interest of public safety
c) For the purpose of public health

3.3.4. CCTV cameras may be used for surveillance as part of a specific investigation or operation other than as an immediate reaction to events. In such circumstances authorisation may either be required by the Council’s Authorising Officer or it may come from the Police or other agencies. Where authorisation is given by the Police it will be authorised in writing by an officer not below the rank of Police Superintendent. A record of this authorisation will be kept and officers must ensure that any surveillance is kept within the terms of this authorisation. copy of the written authorisation will be provided to CoLC for review by CoLC Legal Services, and authorisation is required prior to commencement of any RIPA operation. Legal Services will keep all information on a central file.

3.4 Human Rights Act 1998

3.4.1 The system will be operated with due regard to the Human Rights Act 1998 and in particular the provisions of Article 8, conveying on an individual the qualified right to respect for his or her private and family life.

3.5 Use of Artificial Intelligence and Facial Recognition

3.5.1 CCTV cameras have Facial Recognition technology incorporated but are not configured within the system for its use.
Artificial Intelligence capability will be used on selected cameras around the city to enable more efficient video playback; ANPR vehicle tracking, virtual tripwires, footfall counters, and to enable use of other tools that will make more effective use of the camera system by increasing CCTV operator efficiency and response times.

3.5.2 All Public Space and Transport Hub, St Marks Shopping Centre, some public parks, residential areas on the edge of the city centre (Park ward, Abbey ward, Carholme ward and Castle ward), some city centre car parks, some

council offices (public areas) and Housing properties, Yarborough Leisure Centre, Birchwood Leisure Centre, Community Centres, CoLC Managed Workspaces, Bracebridge Heath recreation field and Forum Centre North Hykeham cameras may employ video analytics/biometrics to assist CCTV operators, for example, by identifying specific colours or patterns in both vehicles and clothing.

Section 4 Accountability and Public Information

4.1 Access and Visits

4.1.1 For reasons of security and confidentiality, access to the CCTV Control Room is restricted in accordance with Section 8 of the Code. However, in the interests of openness and accountability, organised visits from outside organisations and groups, external partners, other CoLC departments and authorised members of the public will be undertaken where possible, but with minimum disruption to the CCTV operation. Such visitors will be reminded of the need for confidentiality. Arrangements for visits will be through the CCTV Team Leader.

4.2 Complaints Procedure

4.2.1 A member of the public wishing to register a concern or complaint with regard to any aspect of the system may do so by contacting the CCTV Team Leader. All complaints shall be dealt with in accordance with the CoLC complaints procedure, a copy of which may be obtained from the CoLC offices or on the website. Complaints will be dealt with and, where necessary, elevated through the following roles:

CCTV Team Leader: 01522 873724 alan.wain@lincoln.gov.uk or alternatively CoLC reception 01522 881188
Community Services Manager:
01522 073690 jonathan.hammond@lincoln.gov.uk
Assistant Director DCE 01522 873421 steve.bird@lincoln.gov.uk

4.3 Accountability

4.3.1 The Director of Communities and Environment being the nominated representative of the system owners, will have unrestricted access to the CCTV control room, as well as The Assistant Director and Community Services Managers

4.3.2 The CCTV Team Leader will have day-to-day responsibility for the system. In the Team Leader's absence, the Community Services Manager takes on day to day responsibility. See Appendix A for key personnel and responsibilities.

4.3.3 Strategic decisions in relation to the CCTV system are subject to the council's formal decision-making structures.

4.3.4 Clearly visible signs will be placed in the locality of the cameras. The signs will indicate:

a) The presence of CCTV monitoring, depicted by an 'Icon' representing a CCTV camera
b) The 'ownership' and controller of the system.
c) The reason for the presence of the CCTV
d) Contact details of the 'data controller' of the system.

Section 5 Assessment of the System

5.1 Evaluation

5.1.1 The CCTV Team Leader will have day to day responsibility for the monitoring, operation and evaluation of the system and the implementation of the Code.

5.1.2 The CCTV Team Leader shall also be responsible for maintaining full management information relating to the incidents dealt with by the Control Room for use in the management of the system and in future evaluations.

5.1.3 The aims and need for cameras is reviewed as part of the DPIA process.

5.1.4 The three yearly review of the Code will ensure that the Code reflects the system and vice versa, and any significant changes will go through the appropriate process prior to adoption.

5.2 Audit

5.2.1 Audit checks undertaken by the CCTV Team Leader will include:

a) Compliance with the Data Protection Legislation, Human Rights Act and RIPA

b) Compliance with the Code

c) Compliance with policy and procedural management of the system

d) Staff compliance with all aspects of the system and their responsibilities under the Code

e) CoLC staff welfare in relation to potentially shocking and upsetting incidents

f) Other audits, which may be in the form of regular spot checks and will include the Control Room records and the content of recorded material.

5.2.2 In addition to the checks carried out and documented, CoLC internal audit section may from time to time conduct an audit of the system's processes, and the records of Lay Visitors (see section 5.2.3 below) will also be recorded.

5.2.3 CoLC operates a Lay Visitors scheme to inspect the system. Full training and guidance on the operation and confidentiality of the system is given to members of this group who are able to visit and inspect the system on a regular basis. These inspections include discussions on system use and interactions with staff, and feedback to the CCTV Team Leader (refer to 4.1).

5.2.4 The operational performance of the scheme is incorporated in the Council's Performance Management arrangements.

Section 6 Staff

6.1 Standards and Accountability

6.1.1 All staff will be subject to a Disclosure and Barring Service check. Staff are Security Industry Authority Licensed.

6.1.2 SIA licensing will also apply to Service Managers that have responsibility for the scheme, in accordance with CoLC interpretation of the current SIA requirements.

6.1.3 Breaches of the Code will be dealt with under the CoLC Disciplinary Policy or Capability Policy as appropriate.

6.1.4 The CCTV Team Leader will have primary responsibility for ensuring that there is no breach of security and that the Code is complied with. The CCTV Team Leader has day to day responsibility for the management of the Control Room and ensuring that systems are in place to ensure that staff comply with all requirements under the Code.

6.1.5 Production of evidential DVD footage for Police, and release of footage to individuals and third parties, will be produced, secured and released in line with the Data Protection Legislation, Human Rights Act, Freedom of Information Act and the National Standard for the release of Data to Third Parties (See Appendix C). All reviews of data will follow the principles of the Code.

6.1.6 All use of the cameras by staff shall be in line with the principles of the Code.

6.1.7 All CCTV staff will be issued with a copy of both this Code and the Operations Procedures Manual and will be required to confirm that they fully understand their obligations and adherence to these documents. They will be fully conversant with the contents of both documents, which may be updated from time to time, and which they will be expected to comply with as far as is reasonably practicable at all times.

6.1.8 CoLC is fully committed to the principles of equality and diversity, and this is an important part of initial training, Ongoing training and quality assurance checks.

6.1.9 No individual will be unjustifiably discriminated against. This includes, but is not limited to, discrimination because of the following characteristics (known as protected characteristics under the Equality Act): Age, Disability, Gender reassignment, Marriage and civil partnership, Pregnancy and maternity, Race, Religion and belief, Sex, Sexual orientation.

6.1.10 Operators will be mindful of exercising prejudices which may lead to the system being used for purposes other than those for which it is intended. Operators may be required to justify their interest in, or recording of, any particular individual, group of individuals or property at any time by virtue of the audit of the system or by the CCTV Team Leader.

6.1.11 No interest will be shown in private dwellings unless as part of an authorised RIPA operation. In addition, the use of cameras will be proportionate to the objectives detailed in the Code. Where the equipment permits it, 'Privacy Zones' will be programmed into the system as required in order to ensure that the interior of any private residential property within range of the system is not surveyed by the cameras. Where such ‘zones’ cannot be programmed operators have been specifically trained in privacy issues. Operators of the system have clear guidelines regarding privacy issues, and any contraventions should be brought to the attention of the CCTV Team Leader as soon as is practicable and the details of the contravention to be recorded in the operator’s incident log.

6.1.12 Any person operating the cameras will act with utmost honesty and decency at all times.

6.1.13 There will be no deliberate monitoring of CoLC employees going about their legitimate CoLC business; except in exceptional circumstances where there is a fear for their health/safety, in respect of an immediate reaction to an offence, or otherwise with the consent of the employee.

6.1.14 In the absence of the CCTV Team Leader the duty operator is responsible for the security of the control room and actions of authorised personnel in the control room. The duty operator must be satisfied that any individual seeking access to the CCTV control room meets the legitimate business criteria as defined in clause 8.1.2.

6.1.15 It is acknowledged and understood that CCTV Operators cannot always deal with every incident that comes to their attention, nor can they proactively pick up every incident that takes place within view of the cameras. Operators are expected to prioritise based on their own experience and training. Operators

will not be criticised for missing or refusing to follow incidents based on decisions reasonably made based on the information available to them and the circumstances at the time.

6.2 Welfare

6.2.1 CoLC will risk assess the potential impacts on staff with regard to the nature and circumstances of their work. Team Leader checks will include reference to potentially disturbing incidents, and Operators will be made aware of the support that is available and encouraged to discuss concerns with the Team Leader or colleagues. CoLC has a policy for dealing with potential trauma events.

Section 7 Control By, and Communication with, Other Schemes, Partners and Organisations

7.1 Operation of the System by the Police

7.1.1 Under extreme circumstances, such as national security, explosions or other localised serious emergencies, the Police may make a request to assume direction of the CCTV system. The Police at a senior level will seek authority from the Chief Executive, prior to Police assuming supervision of the CCTV Control Room for the duration of the incident. Any request and approval will be accepted verbally or in writing. A verbal request or approval will be supported in writing as soon as is reasonably practicable.

7.1.2 In the event of such a request being permitted, the Control Room will continue to be staffed, and equipment only operated by, those personnel who are authorised to do so, and who fall within the terms of Sections 6 and 7 of the Code. The incident log should record the date and time Police assumed responsibility for the CCTV control room and the date and time the Police handed back control to CoLC.

7.2 Communication with Other Schemes and Partners

7.2.1 The control room is linked to a number of related schemes that provide and receive reports concerning activity within the Area. These links are defined as:

7.2.1a A City Centre radio link has been established in the city by the CoLC. Operated by the Business Improvement Group (BIG), membership is open to businesses operating within the system area. Full training is provided by Lincoln BIG.

7.2.1b CoLC car parks, DWP, Public Toilet staff have a radio link. The training on correct radio protocols is undertaken by the department responsible for the staff using the radio link.

7.2.1c Lincolnshire Police Communication Centre is directly contactable by telephone from the CCTV Control Room. There is also a live video link located in the CCTV Control Room enabling operators to transmit camera images to Force Control. Images can be sent through to Lincolnshire Police Communications Centre, in line with the Data Sharing Agreement between Lincolnshire Police and CoLC. The Police radio system base unit is installed in the CCTV control room, this provides two-way radio communications between Lincolnshire Police and the CCTV Control Room, subject to agreed protocols.

7.2.2 Lincolnshire Police will assign a City Centre NPT Sargeant with the necessary seniority to positively engage with the CCTV service and to respond to issues raised surrounding the scheme and Police use of or interaction with CCTV.

7.2.3 In all cases scheme members are aware of the requirement for confidentiality and sign a statement to confirm they will conform to the rules and regulations of the appropriate scheme.

7.2.4 No information received through any of the communication schemes in place shall be shared or passed to any organisation that is not a current member of the relevant schemes or party to a relevant Information Sharing Agreement.

7.2.5 Referrals using any of the listed schemes will be kept short and all parties will maintain a professional approach. Only activity that raises a concern that a member genuinely believes may escalate into a reportable activity such as a public safety issue or criminal act may be referred over a link.

7.2.6 Names may be used where quick identification is necessary; otherwise, a short description of the individual is more appropriate. Under no circumstances are relationships, (other than known relevant criminal connections) or personality (unless the individual is prone to violence) be discussed openly over any of the links, except the Police Airwaves Radio.

7.2.7 Any breach of confidentiality or inappropriate use of any link will automatically result in termination of membership of the scheme for the party responsible until it can be evidenced that necessary steps have been put in place to ensure future security.

7.3 Maintenance of the System

7.3.1 To ensure the system continues to operate effectively and in line with the Aims of the scheme the system shall be subject to a maintenance agreement. The contractual arrangements for the agreement shall make clear the need for confidentiality and the protection of data which the maintenance organisation may come in to contact with through their work with the CoLC CCTV system.

Section 8 Access to and Security of Control Room and Associated Equipment

8.1.1 Only authorised personnel will operate the equipment located within the CCTV Control Room (or equipment associated with the system).

8.1.2 Only those people who have legitimate business related to CCTV will be permitted to enter the CCTV control room. Entry to the CCTV control room will mean acceptance that anything witnessed whilst in the room is confidential (A notice to this effect is posted on the door. See Appendix E). A person entering the room who is not a member of CoLC staff or CCTV maintenance staff attending for known maintenance purposes, will be asked to sign an entry logbook that will show arrival and departure times.

8.1.3 Group visits will require authorisation through a formal booking, in advance, through the Team Leader. All group bookings will have a lead organiser recorded whose full contact details will be provided to the Team Leader and recorded on a data sheet.

8.1.4 While on shift a duty operator will be at their station in the control room unless called away for other work duties or rest reasons. If the duty operator has to leave the control room unattended for any reason, they will ensure that the room is secured so as to prevent unauthorised access. If the duty operator has no option but to leave the control room whilst another person, who is not CCTV staff, is present, they will ensure that this is recorded in the operator's incident log.

8.1.5 CCTV Lay Visitors may visit without prior warning, although for practical purposes (to ensure minimal disturbance to the service and to ensure they can speak with the Team Leader or other management if required) they are encouraged to plan visits in advance with the Team Leader. Lay Visitors are required to sign into the Control Room.

Section 9 Management of Recorded Material

9.1 Control of Recorded Data

9.1.1 For the purposes of the Code 'recorded material' means any material recorded by, or as the result of, technical equipment which forms part of the system.

9.1.2 Every digital recording obtained by using the system has the potential of containing material that can, at any point during its lifespan, be admitted in evidence.

9.1.3 The public must have total confidence that information recorded about their ordinary everyday activities by virtue of the system, will be treated with

due regard to their individual right to privacy in relation to their personal and family life.

9.1.4 It is therefore of the utmost importance, and irrespective of the means or format of the images obtained from the system, that images are treated strictly in accordance with the Code and the Operations Procedures Manual from the moment they are received by the control room until their final destruction. Every movement and usage will be recorded.

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

9.1.6 As a matter of course, recorded material will not be sold or otherwise released to be used for commercial purposes or for the provision of entertainment. In exceptional circumstances the CLC may decide to release footage into the public domain, but this will only be done where the Chief Executive is content there is a wider public benefit. The decision to release footage under this clause is only at the discretion of the Chief Executive, or persons delegated with their authority.

9.2 Release of Data to a Third Party

9.2.1 All data released to third parties will be documented, and the appropriate authority attained. The process for releasing data to Lincolnshire Police officers is set out in the Operations Procedures Manual. All requests for data by Lincolnshire Police must be authorised by an officer of Sergeant ranking or above.

9.2.2 All other requests for data will be channelled through the CCTV Team Leader, who will ensure the principles contained within National Standard for the Release of Data to Third Parties (appendix C) are followed at all times.

9.2.3 In compliance with this standard, it is intended, as far as is reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles:

1) Recorded material shall be processed lawfully, fairly and in a transparent manner and used only for the purposes defined in the Code
2) Access to recorded material will only take place in accordance with the Code
3) The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

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

9.2.5 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 Operations Procedures Manual.

9.2.6 It may be beneficial to make use of footage for the training and education of those involved in the operation and management of the system, and for those involved in the investigation, prevention and detection of crime. Material recorded by virtue of the system may be used for such bona fide training and education purposes.

9.2.7 CoLC does not currently charge for the production and release of footage, but this may be subject to review, and any changes will be in accordance with CoLC policy.

9.3 Recording and Retention Policy

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

9.3.2 Footage will be retained and automatically deleted after 15 days, Body Worn Video for 30 days (or other such period as shall be deemed appropriate, taking into account proportionality in terms of the Data Protection Legislation and service efficiency). Any changes to the retention period will be authorised by the Portfolio Holder.

9.3.3 Footage in relation to an incident must therefore be requested within 15 days (or the standard retention period of the time) and for Body Worn Video within 30 days. Such footage will then be retained for collection by the appropriate authority.

9.3.4 CCTV Operators may themselves choose to save footage, in the absence of a request, if they have reason to believe the footage is or could become significant, and in such circumstances should advise the Team Leader at the earliest opportunity.

9.3.5 Footage requested by, or offered to, an authority, and not collected will be disposed of after a reasonable amount of time (currently 30 days). In the case of significant incidents, a check will be made with the requesting authority prior to deletion.

9.3.6 Once evidence has been collected by the requesting authority, it will be deleted from the CoLC records seven days later, allowing a seven-day period for the receiving organisation to check the footage has transferred successfully to their own system.

9.3.7 With reference to 9.2.6 above, footage may be retained, at the decision of the Team Leader, for training purposes.

Appendices

Appendix A Key Personnel and Responsibilities

1. System Owners
City of Lincoln Council

Responsibilities:
CoLC is the 'owner' of the system. The Director of Communities and Environment will be the single point of reference on behalf of the system owners with responsibility to:

i) Ensure the provision and maintenance of all equipment forming part of the system is in accordance with contractual arrangements which the owners may from time to time enter into.
ii) Maintain close liaison with the CCTV Team Leader.
iii) Ensure the interests of the owners and other organisations are upheld in accordance with the terms of the Code.
iv) Agree to any proposed alterations and additions to the system, the Code and/or the Operations Procedures Manual.

2. System Management
The CCTV Team Leader is responsible for the day-to-day operational management of the system.

The management structure in the event of absence or for escalating issues is:

Community Services Manager
Assistant Director
Strategic Director

Responsibilities*:*
The CCTV Team Leader has delegated authority for data control on behalf of the 'data controller.' Their role includes responsibility to:

i) Maintain day to day management of the system and staff.
ii) Accept overall responsibility for the system and for ensuring that the Code is complied with.
iii) Maintain direct liaison with the owners of the system.
iv) Maintain direct liaison with operating partners.

The Community Services Manager is the Information Asset Owner and fulfils the duties required by IAOs within the CoLC policy and procedures.

The CCTV Service falls within the portfolio of Reducing Inequality.

Appendix B Extracts and Principles of the Data Protection Legislation

Principles:

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

Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the Data Protection Legislation.

For more detail on each principle, please read paragraph 3.2.4 of this Code.

Why are the principles important?

The principles lie at the heart of the Data Protection Legislation. They are set out in both the Data Protection Act 2018 and the UK GDPR. They do not give hard and fast rules, but rather embody the spirit of the data protection regime - and as such there are very limited exceptions.

Compliance with the spirit of these key principles is therefore a fundamental building block for good data protection practice. It is also key to compliance with the Data Protection Legislation.

Failure to comply with the principles may lead substantial fines. Article 83(5)(a) of UK GDPR states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of up to €20 million, or 4% of your total worldwide annual turnover, whichever is higher.

Note: These extracts are for initial direction and guidance only. To ensure compliance with the legislation the relevant Data Protection legislation should be referred to in its entirety.

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

1. Introduction

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 honesty and decency at all times, but they must be used in a manner which stands up to scrutiny and is accountable to the very people they are aiming to protect.

CoLC is committed to the belief that everyone has the right to respect for his or her private and family life and their home.

Any requests for the release of data to third parties will be dealt with in accordance with and in line with all relevant legislation.

2. General Policy

All requests for the release of data shall be processed in accordance with the Code. All such requests shall be channelled through the Data Controller although day to day responsibility may be devolved to the System Manager (CCTV Team Leader).

3. Primary Request to View Data

a) Primary requests to view data generated by a CCTV system are likely to be made by third parties for any one or more of the following purposes:
   - i) Providing evidence in criminal investigations or proceedings
   - ii) Providing evidence in civil proceedings or tribunals but only where directly affecting the Council.
   - iii) The prevention of crime
   - iv) The investigation and detection of crime (may include identification of offenders)
   - v) Identification of witnesses

b) Third parties, which are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:
   - i) Police
   - ii) Statutory authorities with powers to investigate and prosecute, (e.g., Customs and Excise, Trading Standards, etc.)
   - iii) Solicitors
   - iv) Plaintiffs in civil proceedings
   - v) Accused persons or defendants in criminal proceedings
   - vi) other agencies such as Insurance Companies,

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

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

d) In circumstances outlined at note (3) below, (requests by plaintiffs, accused persons or defendants) the data controller, or nominated representative, shall:
i) Be satisfied that there is no inconsistency with any data held by the Police in connection with the same investigation.
ii) All such enquiries are to be processed by all parties in accordance with the Data Protection Legislation.

Notes

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

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

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

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

(5) The data controller can refuse an individual request to view if insufficient or inaccurate information is provided. A search request should specify location and times with 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, the data controller shall ensure that:

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

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

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

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

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 Sergeant. 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 wellbeing, 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

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

i) The request is made in writing or by any other means.

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

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

iv) The person making the request is only shown information relevant to that particular search and which contains personal data of her or himself only, unless all other individuals who may be identified from the same information have consented to the disclosure.

b) In the event of the data controller complying with a request to supply a copy of the data to the subject, only data pertaining to the individual should be copied, (all other personal data which may facilitate the identification of any other person should be concealed or erased). This can only be supplied if a still Image (photo) is required as CoLC does not have redaction software.

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

d) In addition to the principles contained within the Data Protection Legislation, the data controller should be satisfied that the data is:
   i) Not currently and, as far as can be reasonably ascertained, not likely to become, part of a 'live' criminal investigation.
   ii) Not currently and, as far as can be reasonably ascertained, not likely to become, relevant to civil proceedings.
   iii) Not the subject of a complaint or dispute which has not been actioned.
   iv) The original data and that the audit trail has been maintained.
   v) Not removed or copied without proper authority.
   vii) 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 which is specific to the search request shall be shown.
d) It must not be possible to identify any other individual from the information being shown, (any such information will be blanked out, 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 should be sent to an editing house for processing prior to being sent to the requester.

7. Media disclosure

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

i) The release of the material must be accompanied by a signed release document that clearly states what the data will be used for and sets out the limits on its use.
ii) The release form shall state that the receiver must process the data in a manner prescribed by the data controller, e.g., specific identities/data that must not be revealed.
iii) It shall require that proof of any editing must be passed back to the data controller, either for approval or final consent, prior to its intended use by the media (protecting the position of the data controller who would be responsible for any infringement of Data Protection Legislation and the system's Code of Practice).
iv) The release form shall be considered a contract and signed by both parties**.**

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, fairly and in a transparent manner 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 – Not used

RESTRICTED ACCESS

All visitors entering this area are required to

complete an entry in the Access Control Log

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

Confidentiality Clause:

In being permitted entry to this area you agree not to divulge any information obtained, overheard or overseen during your visit.
An entry accompanied by your signature in the Access Control Log is your acceptance of these terms

Please note it is a criminal offence for a person to knowingly or recklessly obtain or disclosure personal data without consent of the controller City of Lincoln Council
(s170 Data Protection Act 2018)

Appendix F The 12 Guiding Principles Protection of Freedoms Act

(Note that the Act was amended in 2022, and this updated the Surveillance Camera Code of Practice required under the Act).

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

Appendix G Regulation of Investigatory Powers Act Guiding Principles

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

The Regulation of Investigatory Powers Act 2000 (which has been significantly amended and updated since, including the Investigatory Powers Act 2016 and the Investigatory Powers (Codes of Practice) Regulations in 2018, amongst other subjects, relates to surveillance by the Police and other agencies (including Local Authorities) and deals in part with the use of directed covert surveillance. Section 26 of this Act sets out what is Directed Surveillance. It defines this type of surveillance as:

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

(a) For the purposes of a specific investigation or a specific operation.
(b) In such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
(c) Otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance.

Although the systems cameras are overt if they are used in such a way that falls within the definition of Directed Surveillance they will only be used if the authorities have been given.

THE COLC SYSTEM CAMERAS WILL NOT BE USED FOR PURPOSES THAT MEET THE DEFINITION OF “INTRUSIVE SURVEILLANCE” UNLESS CORRECTLY AUTHORISED.

The impact for staff in the Police control rooms and CCTV monitoring centres, is such 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.

In the case of authorities given by the Police these are usually authorised by a Superintendent or above. However, if an authority is required immediately, an Inspector may authorise the surveillance. The forms in both cases must indicate the reason and should fall within one of the following categories:-

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

(a) 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.

RIPA also makes provision for directed surveillance to be conducted by a Local Authority. In such cases, the written authority to carry out directed surveillance using the CoLC CCTV system will only be given at Director level providing the permission for such authority has been granted by a magistrate in accordance with the provision of the Protection of Freedoms Act 2012

APPENDIX H - GLOSSARY OF TERMS
Basic CCTV Terminology

CCTV:	A closed circuit television system, not for general public broadcasting
Digital Video Recorder:	A method of recording information digitally initially onto a hard disk which can be retrieved or downloaded to another recording media such as tape, DVD or CD. It retains quality better than analogue recorders.
Data Protection Legislation:	The Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), the Data (Use and Access) Act 2025 and any other applicable implemented Legislation as amended from time to time.
DPIA:	Data Protection Impact Assessment is a process to help identify and minimise data protection risks, in this case in relation to the presence of CCTV cameras.
Dummy Camera:	Looks like a working camera but not capable of recording (or deliberately not recording).
DVD:	Digital Versatile Disc. A data encoding standard for CD-ROM-like discs, capable of storing data at the higher densities needed for recording movies. A typical DVD contains 4.7 Gigabytes of data, and can record approximately 90 minutes of video footage
Fibre Optic:	An efficient method of transmitting video etc. over distances using fibre optic cable. Constructed using thin fibres of glass and laser light technology and

	encased in armour cabling to protect the delicate fibres
Hard Disk Drive:	Electromechanical device used to store large amounts of digital data. They are the most common storage medium used in digital video recorders.
Hard wired:	A single or multi-core cable used to pass video and telemetry signals usually on short runs. E.g., coaxial or fibre optic cables.
HRA 1998:	An act of law introduced to uphold certain rights of the public such as article 6 a right to a fair trial and article 8 a right to a private and family life, full endorsed and adhered to by CoLC.
Information Commissioners Office (ICO)	Principles and requirements of the Data Protection Legislation, codes of practice and key themes, such as CCTV, Artificial Intelligence and children.
Infra-Red:	A range of frequencies just below the human visible spectrum. It is used for transmitting information or providing additional illumination for cameras. Used to enhance CCTV images where there is little or no artificial light e.g., Works depots or public parks
IP camera:	A type of CCTV camera that outputs video as digital information usually according to the TCP/IP protocol.
Operator:	The person designated to operate the surveillance system
Privacy Zone:	Usually electronically programmed into the CCTV system to stop accidental intrusion with the cameras into private residential widows and other areas regarded as private

Pre-set:	A function programmed into the control to allow a camera to move to a pre-set position following an alarm or physical activation (its default position)
RIPA 2000:	Regulation of Investigatory Powers Act 2000, a law allowing the surveillance of people in private and public places.
SIA:	The Security Industry Authority. A government department set up as a result of the Private Security Act 2001 with responsibility for the licensing of individuals working in the security industry including CCTV operators The office of the commissioner was created under the Protection of Freedoms Act 2012 to further regulate CCTV. The act required a code of practice to be produced about surveillance camera systems. The role of the Surveillance Camera Commissioner is to encourage compliance with the Surveillance Camera Code of Practice.
Wireless:	A means of transmission of CCTV data without use of wires or cables, e.g., by using radio waves or microwaves.