West Lindsey
CCTV & Monitoring

Code of Practice

Contents

1. Introduction and Definitions

1.1 Introduction

West Lindsey District Council provides monitored CCTV services for the benefit of the wider public, partner agencies and customers. We use the latest in CCTV technology to deliver high quality surveillance that keeps people, property and assets safe.

Our CCTV Control Centre monitors and records all footage from our camera network. With direct communication links to the police and other agencies we use camera footage to prevent and detect incidents of crime, public disorder, anti-social behaviour, theft and more.

This Code of Practice applies to the operation of our CCTV Service.

1.2 Ownership

The CCTV Service is owned by West Lindsey District Council who is responsible for the management, administration and security of the system. The Council will ensure the protection of individuals and the public by complying with this Code of Practice.

1.3 CCTV Service Purpose

We create safety by providing CCTV Services for people, partners and businesses. The Council is committed to providing services in line with the most current British Standards and the Surveillance Camera Commissioner's CCTV Code of Practice.

1.4 Code of Practice Purpose

To inspire public confidence by ensuring that all public area CCTV systems which are linked to the CCTV Service are operated in a manner that will secure their consistent effectiveness and preserve the civil liberty of law abiding citizens at all times.

The Code of Practice ensures the Council complies with British Standards for CCTV Monitored Services in public places and meets the 12 Principles of CCTV as detailed in the Surveillance Camera Commissioner's CCTV Code of Practice.

The Code of Practice is reviewed annually to ensure continued compliance with all standards, codes and best practice nationally.

1.5 Definitions

1.5.1 **CCTV Control Centre** shall mean the secure area of a building where CCTV is monitored and where data is retrieved, analysed and processed. It is also the location where radio systems are controlled and accessed.

1.5.2 **CCTV Service** shall mean the totality of the arrangements for CCTV in the locality and is not limited to the technological systems, staff and operational procedures.

1.5.3 **GDPR** is the General Data Protection Regulations and **DPA 2018** is the Data Protection Act 2018.

1.5.4 **CCTV system** means the surveillance items comprising cameras and associated equipment for monitoring, transmission and controlling purposes.

1.5.5 **Data** shall mean all information, including that about a person in the form of pictures, and any other associated linked or processed information.

1.5.6 **Personal Data** shall mean any data which related to a living individual who can be identified:

a) From that data
b) From that data and other information which is in the possession of or is likely to come into the possession of, the data controller

1.5.7 **Sensitive personal data** is personal data which is deemed to be sensitive such as bio-metric data (images) when used for ID purposes. The most significant of these, for the purposes of this code are information about:

a) The commission or alleged commission of any offences
b) Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

1.5.8 **An Incident** is an activity that raises cause for concern that the safety or security of an individual or property including vehicles that me be compromised or that an offence has been, is being or is about to be committed, or that an occurrence has taken place warranting specific action by an operator.

1.5.9 **The Owner** is West Lindsey District Council, the organisation with overall responsibility for the formulation and implementation of policies, purposes and control of the service.

1.5.10 **The Manager** has the responsibility for the implementation of the policies, purposes and methods of control for the CCTV Service.

1.5.11 **Data Controller** means a person who (either along or jointly or in common with other persons) determines the purposed for which and the manner in which any personal data are or are about to be processed.

1.5.12 **Contractor** is a party contracted by the owner to undertake the day to day operation of their CCTV system, either utilising the owner's facilities or supplying a full monitoring service.

1.5.13 **Operators** work in the CCTV Control Centre and carry out the physical operation of controlling the CCTV system and the data generated. All operators are screened, trained and licensed to required standards.

1.6 System Description

1.6.1 The CCTV systems referred to in this document operate in the West Lindsey District Council area. Whilst the service is owned by the Council, it's implementation and/or expansion is supported by the following bodies:

- Lincolnshire Police
- Gainsborough Town Council
- Market Rasen Town Council
- Local Businesses
- Local Charities

The owner, contractors, operators and all partners will work in accordance with this Code of Practice. The partners will have no involvement in the operating of the system with the exception of the Police and authorised and trained personnel.

1.6.2 This Code of Practice shall apply to CCTV systems known as the West Lindsey CCTV Service.

1.6.3 The system consists of static and fully functional (pan, tilt and zoom) cameras and either a fibre optic or wireless transmission system which sends pictures to the Control Centre.

1.6.4 Images from all cameras are recorded simultaneously 24 hours and 365 days each year.

1.6.5 The system has a dedicated CCTV transmission link to local police stations and Police Control Rooms where live pictures and events can be monitored.

1.6.6 The physical and intellectual rights in relation to any and all material recorded within the Control Centre shall at all times remain the ownership of the Council.

1.6.7 The system includes the use of deployable CCTV cameras which can be used for specific time periods in areas subjected to or at risk of crime. Images on deployable cameras shall only record at agreed key times to meet the deployment need.

2. Changes to the Code of Practice

2.1 Consultation

Any major changes to this Code of Practice will take place only after consultation with the relevant management group and upon agreement of all organisations with a participatory role in the operation of the CCTV Service.

2.1.1 Major changes to this Code of Practice are defined as changes that affect its fundamental principles and shall be deemed to include:

a) Significant legal implications
b) Matters which have privacy implications
c) Additions to permitted uses criteria (e.g. purposes of the service)
d) Changes in the right of access to personal data, except statutory requirements

2.1.2 Minor changes to this Code of Practice are defined as operational and procedural matters which do not affect the fundamental principles and purposes. These include:

a) Additions and omissions of contractors
b) Additional clarifications, explanations and corrections
c) Additions in order to conform to the requirements of any statutory Acts and changes in criminal legislation

A minor change may be agreed between the Manager and owner of the service. This Code of Practice will be subject to annual review which will include compliance with the relevant legislation and standards.

2.2 Supplementary Documentation

This Code of Practice will be supplemented by the following documents:

a) CCTV Operations Manual
b) Operators Equipment Manual

Each document contains instructions and guidance to ensure that the objectives and principles set out in this document are achieved. These documents will be restricted to the staff and authorised partners.

3. Purpose of the Code of Practice and CCTV Service

3.1 Purpose of and Compliance with the Code of Practice

3.1.1 This Code of Practice is to detail the management, administration and operation of the CCTV Service and the associated Control Centre.

3.1.2 The Code of Practice has a dual purpose, in that it will assist owners, management and operators to understand their legal and moral obligations whilst reassuring the public about the safeguards contained within it.

3.1.3 The owners, CCTV Operators and users of the CCTV systems and associated safety and security equipment connected to the Control Centre shall be required to give a formal undertaking that they will comply with this Code of Practice and act in good faith with regard to the basic principles contained within it.

3.1.4 The owners, CCTV Operators, users and any visitors to the Control Centre will be required to sign a formal confidentiality declaration that they will treat any viewed and/or written material as being strictly confidential and that they undertake not to divulge it to any other person.

3.2 Purpose of the CCTV Service

We will use CCTV systems to:

a) Make West Lindsey a safe and clean place in which to live, work and visit

b) Reduce anti-social behaviour, drug and alcohol misuse and provide public reassurance

c) Gain evidence of environmental crimes such as graffiti, vandalism, littering, fly-tipping and dog fowling

d) Ensure that traffic flows easily and safely on the road network

e) Provide traffic management support and gain evidence for the enforcement of moving traffic offences

f) Provide assistance and direction in the event of any emergency incident

g) Support police investigations and civil investigations when appropriate

h) Ensure the safety and security of Council and partner agency assets

4. Fundamental Principles and Policies

4.1 Rights of Privacy

West Lindsey District Council and partners support an individual's right to privacy and will insist that all agencies involved in the provision and use of public surveillance CCTV systems connected to the Control Centre accept this fundamental principle as being paramount.

4.2 Principles of Management of the Service

4.2.1 Prior to the installation of cameras an 'Impact Assessment' to determine whether CCTV is justified and how it will be operated will be undertaken in compliance with the Surveillance Camera Commissioners CCTV Code of Practice.

4.2.2 Cameras will be sited to ensure that they can produce images of the right quality, taking into account technical and environmental issues.

4.2.3 The operational requirements of the system will be considered at the time of completing the 'Impact Assessment' for each proposed camera to determine the quality of images required.

4.2.4 Sufficient safeguards and encryption will be used for wirelessly transmitted data to protect from unauthorised access.

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

4.2.6 Operators are aware of the purpose(s) for which the Service has been established and that the CCTV equipment is only used to achieve the identified purposes.

4.2.7 The service will be operated with due regard for the privacy of the individual.

4.2.8 Before cameras are placed in residential areas the residents in that area will be informed or consulted concerning the proposed system.

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

4.2.10 All operators will hold the relevant Disclosure and Barring Service certificate, Police vetting and Security Industry Authority (SIA) as required.

4.3 Policy of the Service and Signage

The service aims to provide surveillance of the public areas within the West Lindsey District Council area in order to fulfil the stated purposes of the service. The area protected by CCTV will be indicated by the presence of signs. The signs will be placed so that the public are aware that they are within an area covered by surveillance equipment. The signs will state the organisation responsible for the Service, the purposes of the Service and a contact telephone number. Data will not be held for longer than necessary and disposal of information will be regulated.

4.4 Point of contact

Should the public wish to make contact with the owners of the service they may write to:

West Lindsey CCTV Service
The Guildhall
Marshall's Yard
Gainsborough
DN21 2NA

4.5 Release of information to the public

Information will be released to third parties, itemised in Section 8 who can show legitimate reasons for access. They will be required to request any information with reasons in writing and identify themselves. Information will only be released if the data captures identifiable individuals or information relating to individuals and the reasons are deemed acceptable, the request and release of information complies with current legislation and on condition that the information is not used for any other purpose than that specified.

Individuals may request to view information concerning themselves held on record in accordance with GDPR. The procedure is outlined in Section 8.9 of this Code of Practice.

4.6 Release of information to statutory prosecuting bodies

The policy is to assist statutory prosecuting bodies such as the Police, and other agencies where it is deemed by the Data Controller that disclosure is to be made in compliance with the exemptions detailed within DPA 2018. Such agencies and prosecuting bodies may have access to information, permitted for disclosure, on application to the owner of the service or the Manager, and provided the reasons and statement of purpose, accord with the objectives of the Service and conditions outlined in section 8.0. The information will be treated as evidential exhibits.

4.7 Annual policy review

There will be an annual policy review covering the following aspects:

a) Whether the purpose and objectives statements remain valid
b) Change in extent of the Service
c) Contracts with suppliers
d) A review of the data protection or legal requirements
e) Maintenance schedule and performance test of the system
f) Service evaluation findings
g) Complaints procedure and evaluation

5. Data Protection Act and other legislation

5.1 Data Protection Registration

The service is registered with the Information Commissioner's Office. The service will be managed in accordance with the principles of the General Data Protection Regulation (GDPR) and DPA 2018.

Article 5 of the GDPR sets our seven key principles. The following is a summary of these principles:

5.1.1 a) Lawfulness, fairness and transparency

Processed lawfully, fairly and in a transparent manner in relation to individuals.

5.1.2 b) Purpose limitation

Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

5.1.3 c) Data minimisation

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

5.1.4 d) Accuracy

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.

5.1.5 e) Storage limitation

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 GDPR in order to safeguard the rights and freedoms of individuals.

5.1.6 f) Integrity and confidentiality

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.

5.1.7 Accountability

The accountability principle requires organisations to take responsibility for what they do with personal data and how they comply with the other principles. We must have appropriate measures and records in place to be able to demonstrate our compliance.

5.2 Data Processing

In order to lawfully process special category data we have identified lawful bases under Article 6 GDPR as listed below:

For CCTV in public spaces:

6(e) The processing is necessary for you to perform a task in the public interest or for your official functions and the task or function has a clear basis in law

For CCTV in private locations or provided through contract:

6(f) The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individuals personal data which overrides those legitimate interests

To process special category data we have also identified the following lawful conditions of Article 9 GDPR:

9(2)(a) Explicit consent
9(2)(b) The obligations of employment, social security and social protection law
9(2)(f) Processing is necessary for the establish, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
9(2)(g) Processing is necessary for reasons of substantial public interest
9(2)(i) Processing is necessary for reasons of public interest in the area of public health

These should be read alongside the DPA 2018 which add more specific conditions and safeguards. Schedule 1.1 contains specific conditions under Article 9(2)(b) and (i). Schedule 1.2 contains specific substantial public interest conditions for Article 9(2)(g).

5.3 Human Rights Act 1998

The system will be operated by or on behalf of a public authority, the authority has considered the wider human rights issues and in particular the implications of the European Convention on Human Rights, Article 8 (the right to respect for private and family life).

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Therefore, to comply with Article 8 (1), and Article 8 (2) the Council will always considers the following contained within this document:

Proportionality - Sections 4.2.1, 4.2.2, 4.2.3 and 4.2.5
Legality - Sections 4.2.6 and 4.2.7
Accountability - Sections 4.2.9 and 4.2.10
Necessity/Compulsion - Section 4.2.3

5.4 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 prosecution of its own case (known as unused material) but disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on the data controller by Section 7 of the Data Protection Act 1998, (known as subject access).

5.5 Freedom of Information Act 2000

If a request for images is received via a FOIA application and the person requesting is the subject, these will be exempt from the FOIA and will be dealt with under The Data Protection Principles.

Any other requests not involving identification of individuals can be disclosed but only if it does not breach the data protection principles.

5.6 Regulation of Investigatory Powers Act 2000

Introduction

The Regulation of Investigatory Powers Act 2000 came into force on 2nd October 2000. It places a requirement on public authorities listed in Schedule 1: Part 1 of the act to authorise certain types of covert surveillance during planned investigations.

Background

General observation forms part of the duties of many law enforcement officers and other public bodies. Police officers will be on patrol at football grounds and other venues monitoring the crowd to maintain public safety and prevent disorder. Officers may also target a crime "hot spot" in order to identify and arrest offenders committing crime at that location.

Trading standards or HM Customs & Excise officers might covertly observe and then visit a shop as part of their enforcement function to verify the supply or level of supply of goods or services that may be liable to a restriction or tax. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve **systematic surveillance of an individual**. It forms a part of the everyday functions of law enforcement or other public bodies. This low-level activity will not usually be regulated under the provisions of the 2000 Act. Neither do the provisions of the Act cover the normal, everyday use of **overt** CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime. However, it had not been envisaged how much the Act would impact on specific, targeted use of public/private CCTV systems by 'relevant Public Authorities' covered in Schedule 1: Part1 of the Act, when used during their planned investigations.

The consequences of not obtaining an authorisation under this Part may be, where there is an interference by a public authority with Article 8 rights (invasion of privacy), and there is no other source of authority, that the action is unlawful by virtue of section 6 of the Human Rights Act 1998 (Right to fair trial) and the evidence obtained could be excluded in court under Section 78 Police & Criminal Evidence Act 1984.

The Act is divided into five parts. Part II is the relevant part of the act for CCTV. It creates a system of authorisations for various types of covert surveillance. The types of activity covered are "intrusive surveillance" and "directed surveillance". Both types of surveillance if part of a pre-planned operation will require authorisation from specified persons named in the Act. In addition, the reasons for such surveillance must be clearly

indicated and fall within the criteria outlined by this legislation. A procedure is in place for regular reviews to be undertaken into authorisation.

The Council and the CCTV Service will observe the criteria laid out in the legislative requirements.

5.7 Surveillance Camera Code of Practice

The Code of Practice was a requirement of the Protection of Freedoms Act 2012 and sets out guidelines for CCTV and Automatic Number Plate Recognition (ANPR) systems to ensure their use is open and proportionate and that they are able to capture quality images that give police a better chance to catch criminals and cut crime.

The code has been built upon 12 guiding principles, which provide a framework of good practice that includes existing legal obligations. Those existing obligations include the processing of personal data under the Data Protection Act 1998, a public authority's duty to adhere to the Human Rights Act 1998 and safeguards under the Regulation of Investigatory Powers Act 2000 associated with the use of directed and covert surveillance by a public authority.

The use of a surveillance camera system must:

1. Always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need
2. Take into account its effect on individuals and their privacy
3. Have as much transparency as possible, including a published contact point for access to information and complaints
4. Have clear responsibility and accountability for all surveillance activities including images and information collected, held and used
5. Have clear rules, policies and procedures in place and these must be communicated to all who need to comply with them
6. Have no more images and information stored than that which is strictly required
7. Restrict access to retained images and information with clear rules on who can gain access
8. Consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards
9. Be subject to appropriate security measures to safeguard against unauthorised access and use

10. Have effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with

11. 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, when used in pursuit of a legitimate aim

12. Be accurate and kept up to date when any information is used to support a surveillance camera system which compares against a reference database for matching purposes.

5.8 Crime & Courts Act 2013

The Crime and Courts Act became law on 1st October 2013 and replaced the Serious Organised Crime and Police Act 2005. CCTV Control Rooms, RVRC's and the like are under Section 7 of the Crime & Courts Act 2013 required by law to share information (CCTV images) to the National Crime Agency (NCA). If a request is received from the NCA then the Council MUST comply with the request and provide the data.

Section 7, Subsection (3) provides information obtained by the NCA in connection with the exercise of any NCA function may be used by the NCA in connection with the exercise of any other NCA function. For example, information obtained in the course of gathering criminal intelligence may be used in connection with NCA's crime reduction function.

Section 7, Subsection (4) provides that the NCA may disclose information in connection with the exercise of any NCA function if the disclosure is for any "permitted purpose" as defined within Section 16(1) of the Act. This would apply in situations where, for example, the NCA has received information on suspected criminal activity (such as a 'Suspicious Activity Report' – which help banks and financial institutions protect themselves and their reputation from criminals and help law enforcement to track down and arrest them) and has decided to share this information with an organisation or person outside the NCA (such as a financial institution) for the purpose of preventing or detecting crime.

NOTE: any information which falls within the scope of RIPA Act 2000 will still require the necessary authority prior to the release of images.

6. Accountability

6.1 Support of Principles

The Council and the Partners support the principle that the community at large should be satisfied that the public surveillance CCTV systems are being used, managed and controlled in a responsible and accountable manner and that in order to meet this objective there will be independent assessment and scrutiny. It is the responsibility of all parties to maintain a continuous review of its integrity, security, procedural efficiency, methods of operation and retention and release of data.

6.2 Hierarchy of Responsibilities

6.2.1 The Owner (West Lindsey District Council)

The owner shall be responsible for policy, effective management and public relations of the Service. They shall produce a written policy and be responsible for its implementation. This shall be carried out in consultation with users of the Service and provide for the release of information relating to the operation of the system. The owner is responsible for dealing with complaints, and ensuring a fair system of staff selection and recruitment is adopted for staff employed in the service. The role of owner also includes all statutory responsibilities including the role of “data controller” as prescribed by the Data Protection Act 1998 Section 1 Subsection 1(1)

6.2.2 The Manager

The Manager or designated member of staff should undertake regular reviews of the documented procedures to ensure that the provisions of this Code of Practice are being complied with. These should be reported back to the owner of the Service. To facilitate this, regular minuted meetings will be held with the Supervisor to go through the points listed below.

The Manager is the person who has direct control of the Service and as such he/she will have authority for the following:

- Staff management
- Observance of the policy and procedural practices
- Release of data to third parties who have legal right to copies
- Control and security clearance of visitors
- Security and storage of data
- Security clearance of persons who request to view data
- Release of new and destruction of old data and tapes

- Liaison with police and other agencies
- Maintenance of recording and monitoring equipment

The Manager should retain responsibility for the implementation of procedures to ensure that the Service operates according to the purposes for which it was installed and in accordance with the objectives identified for the Service.

The Manager shall also ensure that on a day-to-day basis all equipment is working correctly and that the operators of the Service comply with the Code of Practice and Procedural Manual. Dealing with breaches of the codes and disciplinary measures shall lie with the Manager.

6.2.3 The Supervisor

The Supervisor has a responsibility to ensure that at all times the Service is operated in accordance with the policy and all procedural instructions relating to the Service, and for bringing to the immediate attention of the Manager any matter affecting the operation of the Service, including any breach or suspected breach of the policy, procedural instructions, security of data or confidentially. In the Managers absence the Supervisor will have responsibility for:

- Staff management
- Release of data to third parties who have legal right to copies
- Control and security clearance of visitors
- Security and storage of data
- Security clearance of persons who request to view data
- Release of new Media
- Liaison with police and other agencies

The Supervisor should ensure that at all times operators carry out their duties in an efficient and responsible manner, in accordance with the objectives of the Service. This will include regular checks and audit trails to ensure that the documentation systems in place are working effectively. These systems include:

- Media logs
- Fault log
- Visitor log
- Log book
- Audit logs
- Witness statements
- The security of data

The Supervisor should ensure operators comply with Health and Safety Regulations.

6.2.4 The Operators

The operators will be responsible for complying with the code of practice and procedural manual. They have a responsibility to respect the privacy of the individual, understand and comply with the objectives of the Service. They are required to be proficient in the control and the use of the CCTV camera equipment, recording and playback facilities, data erasure, and maintenance of all logs. The information recorded must be accurate, adequate and relevant to the purpose of the Service. They should bring to the attention of the CCTV maintenance contractor immediately any equipment defect that may occur.

6.2.5 Contractor's Responsibilities

There are a number of contractors responsible for Maintenance of CCTV equipment. The response provided by contractors is subject of a written contract and records of responses are maintained.

6.3 Accountability

The Manager shall be accountable to the owner of the Service and will provide periodic progress reports on the Service. The Manager will resolve technical matters. The Manager or Supervisor will resolve operational matters.

Failure of the operators to comply with the procedures and code of practice should be dealt with by the Manager or Supervisor. Person(s) misusing the Service will be subject to disciplinary or legal proceedings in accordance with the Councils employment policy or contractor contract arrangements.

6.4 Audit

Regular independent random audits will check the operation of the service and the compliance with the code of practice. It will consider the following:

- The level of attainment of objectives and procedures
- Random audits of the data log and release of information
- The review policy
- Standard costs for the release of viewing of material
- The complaints procedure

6.5 Complaints

A member of the public wishing to make a complaint about the service may do so through West Lindsey District Councils complaint procedure. Copies of the complaints procedure are available to view on the Council's website.

A report on the numbers of complaints will be collated by the Manager or designated member of staff in order to assess public reaction to, and opinion of,

the use of the Service. The annual report will contain details of the numbers of complaints received, the time taken to acknowledge and respond to complaints, the method of receiving and handling complaints and the degree of satisfaction in handling complaints.

6.6 Personnel

6.6.1 Security screening

All personnel employed to control/operate or manage the Service are or will be security screened in accordance with British Standard 7858: *Code of practice for screening of personnel in a security environment.* In addition, they will also be subject to vetting to none police staff anti-terrorist security screening standards.

6.6.2 Training

Where necessary operators are or will be trained to the criteria required by the private Security Industry Act 2001 and licensed by the Security Industry Authority for Public Space Surveillance systems.

All staff are trained to the highest available standard. Training and annual refresher training includes:

- The use of all appropriate equipment
- The operation of the systems in place
- Terms of employment of the Council or Third Parties
- The disciplinary policy of the Council or Third Parties
- Recognise and understanding privacy and disclosure issues
- All relevant legal issues including Data Protection and Human Rights
- The management of recorded material including requirements for handling and storage of material needed for evidential purposes

6.6.3 Contractor's

There are special condition's imposed upon contractor's carrying out works on the system. These are detailed in the Procedural Manual. Wherever possible CCTV installation and maintenance contractors should not have sight of any recorded data.

7. Control Centre Management and Operation

7.1 Access to Control Centre

Access to the Control Centre will be strictly controlled and the security of the facility shall be maintained at all times. Only those persons with a legitimate purpose will be permitted access to the control and monitoring Room.

The Manager or in his/her absence the Supervisor, is authorised to determine who has access to the Control Centre. This will normally be:

- Operating staff
- The Manager and Supervisor
- Police officers requiring to view footage of an incident, or collecting/returning media being considered for intelligence or evidential purposes. These visits will take place by prior appointment only.
- Engineers and cleaning staff
- Independent Inspectors appointed under this Code of Practice may visit the control room without prior appointment
- Organised visits by authorised persons in controlled circumstances

All visitors to the Control Centre, including Police Officers, will be required to sign a visitors log and a declaration of confidentiality.

7.2 Response to an incident

7.2.1 The Procedural Manual details:

a) What action should be taken
b) Who should respond
c) The time scale for response
d) The times at which the observation should take place

7.2.2 A record of all incidents will be maintained in the incident log. Information will include anything of note that may be useful for investigative or evidential purposes.

7.3 Who makes the response and the time scale

Incidents of a criminal nature will be reported to the appropriate Police Force. The response will be made by the Police Service in accordance with their policies.

7.4 Observation and recording of incidents

Recording will be throughout the 24 hour period in time lapse mode. Wherever possible the Service will be monitored 24 hours a day. In the event of an incident being identified there will be particular concentration on the scene.

7.5 A successful response

7.5.1 The criteria for measuring a successful response are:

a) A good observational record of the incident
b) A short time scale for response to the incident
c) Identification of a suspect
d) The prevention or minimisation of injury or damage
e) Reduction of crime and disorder
f) Improving public safety
g) Restoration of tranquillity

7.6 Operation of the System by the Police

There is a live feed monitor installed at specific Police Stations and the Police Control Rooms. Under certain circumstances the Police may make a request to view a number of cameras to which this Code of Practice applies. The Police communications Supervisor will provide sufficient information to the operator of the genuine need for such surveillance.

In the event of the police requesting use of the equipment from within the CCTV Control Centre to monitor situations, the Control Centre will continue to be staffed and equipment operated by, only those personnel who are authorised to do so and who fall within the terms of this Code.

In very extreme circumstances such as a major incident a request may be made for the Police to take total control of the system in its entirety, including the staffing of the Control Centre and personal control of all associated equipment; to the exclusion of all representatives of the system owners. A request for total exclusive control must be made in writing by a Police Officer not below the rank of Superintendent (or designated deputy).

Once the police undertake any of the above they become responsible under the Data Protection Act 2018.

Telephone and Police radio systems are used to effectively relay information on incidents that arise. All radio systems are licensed and appropriate procedures are followed for their secure use.

8. Privacy and Disclosure Issues

8.1 Privacy

Cameras should not be used to infringe an individual's rights of privacy. The cameras generally are sited where they will not be capable of viewing the internal areas of residential properties. If it is found there is a possibility that cameras would intrude in private areas, privacy zones may be programmed into the cameras where possible and CCTV operators trained to recognise privacy issues.

8.2 Disclosure Policy

8.2.1 The following principles must be adhered to:

a) All employees will be aware of the restrictions set out in this Code of Practice in relation to access to, and disclosure of, recorded images

b) Images not required for the purposes of the service will not be retained longer than necessary. However, on occasions it may be necessary to retain images for longer periods, where a law enforcement body is investigating a crime to give them the opportunity to view the images as part of an active investigation.

c) The Data controller will only disclose to third parties who intend processing the data for purposes which are deemed compatible with the objectives of the CCTV Service

d) Monitors displaying images from areas in which individuals would have an expectation of privacy will not be viewed by anyone other than authorised employees of the user of the equipment

e) Recorded material will only be used for the purposes defined in the objectives and policy

f) Access to recorded material will be in accordance with policy and procedures

g) Information will not be disclosed for commercial purposes and entertainment purposes

h) All access to the medium on which the images are recorded will be documented

i) Access to recorded images will be restricted to those staff who need to have access in order to achieve the purpose(s) of using the equipment

j) Viewing of the recorded images should take place in a restricted area

8.2.2 Before data is viewed by a third party the Manager or Supervisor should be satisfied that data is:

a) The subject of a complaint or dispute that is unanswered

b) The original data and the audit trail is maintained throughout

c) Not part of a current criminal investigation by Police, or likely to be so

d) Not part of a civil proceeding or likely to be so

e) Not removed or copied without proper authority

f) The image obtained is aimed at identifying individuals or information relating to an individual

8.3 Access to recorded images

Access to recorded images will be restricted to the Manager or designated member of staff who will decide whether to allow requests for access by third parties in accordance with the disclosure policy.

8.4 Viewing recorded images

Viewing of recorded images should take place in a restricted area. Other employees should not be allowed to have access to that area when viewing is taking place.

8.5 Operators

All operators are trained in their responsibilities in relation to access to privacy and disclosure issues. All operators are required to sign a Confidentiality Statement to work in the Control Centre.

8.6 Removal of media for viewing

The removal of media on which images are recorded, for viewing purposes, will be documented in accordance with Data Protection principles and the procedural manual.

8.7 Access to data by third parties

8.7.1 Access to images by third parties will only be allowed in limited and prescribed circumstances. For this service disclosure will be limited to the following:

a) Law enforcement agencies where the images recorded would assist in a specific criminal enquiry

b) Prosecution agencies

c) Legal representatives

d) The media, where it is assessed by the Police that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that assessment the wishes of the victim of an incident should be taken into account.

e) The people whose images have been recorded and retained (Data Subject) unless disclosure to an individual would prejudice criminal enquiries or criminal proceedings.

f) Where the relevant legislation allows access

g) Public bodies that wish to pursue civil cases

h) CCTV Service customers in accordance with this document and any customer service agreement

8.7.2 All requests for access or for disclosure will be recorded. If access or disclosure is denied, the reason shall be documented.

8.7.3 If access to or disclosure of the images is allowed, details shall be documented.

8.7.4 Recorded images should not in normal circumstances be made more widely available, for example, they should not be routinely made available to the media or placed on the internet.

8.7.5 If it is intended that the images will be made more widely available, that decision should be made by the Manager or designated member of staff and the reason documented.

8.7.6 The owner should not unduly obstruct a bone fide third party investigation to verify the existence of relevant data.

8.7.7 The owner should not destroy data that is relevant to a previous or pending search request which may become the subject of a subpoena.

8.7.8 The owner should decide which other agencies, if any, should have access to data and it should be viewed live or recorded but a copy should never be made or released.

8.8 Disclosure in the public interest

Requests to view personal data that do not fall within the above categories but that may be in the public interest should be considered. Examples may include public health issues, community safety or circumstances leading to the prevention or detection of crime. Material released to a third party for the purposes of crime prevention or detection, should be governed by prior written agreement with the Chief Constable.

Material may be used for bona fide training such as Police or staff training.

8.9 Data subject access disclosure

8.9.1 All staff involved in operating the equipment must be able to recognise a request for access to recorded images by data subjects and be aware of individual's rights under this section of the Code of Practice.

8.9.2 Data subjects requesting access will be provided with a Subject Access Request Form and Guidance Notes describing the types of images recorded and retained and the purposes for recording and retention.

8.9.3 Subject access rights are governed by the General Data Protection Regulation (GDPR) and include the following provisions:

a) Person gives sufficient and accurate information about a time and place

b) Information required as to the identification of the person making the request

c) The Data Controller only shows information relevant to the search

8.9.4 If a copy is requested, it will be necessary to ascertain whether the images obtained are aimed at learning about the Data Subjects activities. If this is not the case and there has been no captured images of identifiable individuals or information relating to individuals then this may not fall within the GDPR and DPA 2018 and access may be denied. Any refusal should be documented

8.9.5 If on the other hand images have been obtain and CCTV used to focus on the activities of particular people either by directing cameras at an individual's activities, looking out for particular individuals or examining recorded CCTV images to find things out about the people in them such as identifying a criminal or a witness or assessing how an employee is performing. These activities will still be covered by the GDPR and DPA 2018.

8.9.6 Only data pertaining to that person is copied unless consent from all third parties is received. The subject access request will be dealt with promptly and in any case within 28 days of receipt of the request or within 28 days of receiving all the information required

8.9.7 All subject access requests should be dealt with by the Manager or designated member of staff.

8.9.8 A search request should provide sufficient information to locate the data requested (e.g. within 30 minutes for a given date and place). If insufficient information is provided a data controller may refuse a request until sufficient information is provided.

8.9.9 Under certain circumstances in compliance with GDPR the Manager or designated member of staff can decide that a subject access request is not to be complied with. In such cases the refusal will be documented.

8.10 Provision of data to the individual

The Manager having verified the validity of a request should provide requested material to the individual. Only that personal data specific to the search request should be provided. Other individuals should be blanked off by electronic screening or manual editing on the monitor screen. As there is no on site means of editing out other personal data the material would have to be sent to an editing house for processing.

If the individual agrees it may be possible to provide subject access by viewing only. If this is the case:

a) Viewing should take place in a controlled environment
b) Material not relevant to the request should be masked or edited out

8.11 Other rights

8.11.1 All staff involved in operating the equipment must be able to recognise a request from an individual to prevent processing likely to cause substantial and unwarranted damage to that individual.

8.11.2 In relation to a request to prevent processing likely to cause substantial and unwarranted damage, the Manager or designated member of staff's response should indicate whether he or she will comply with the request or not.

8.11.3 The Manager or designated member of staff must provide a written response to the individual within 21 days of receiving the request setting out their decision on the request.

8.11.4 If the Manager or designated member of staff decide that the request will not be complied with, they must set out their reasons in the response to the individual.

8.11.5 A copy of the request and response will be retained.

8.12 Media Disclosure

Disclosure of images from the CCTV Service must be controlled and consistent with the purpose for which the Service was established. For example, if the Service is established to help prevent and detect crime it will be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated, but it would not be appropriate to disclose images of identifiable individuals to the media for entertainment purposes or place them on the internet. Images can be released to the media for identification purposes; this will not generally be done by anyone other than a law enforcement agency.

9. Recorded Material Management

9.1 Retention of Images

Images, which are not required for the purpose(s) for which the equipment is being used will not be retained for longer than is necessary. As mentioned previously, on occasions, images may need to be retained for longer periods as a requirement of an investigation into crime. While images are retained access to and security of the images will be controlled in accordance with the requirements of the GDPR and DPA 2018.

9.1.1 Recorded material should be of high quality. In order for recorded material to be admissible in evidence total integrity and continuity must be maintained at all times.

9.1.2 Security measures will be taken to prevent unauthorised access to, alteration, disclosure, destruction, accidental loss or destruction of recorded material.

9.1.3 Recorded material will not be released to organisations outside the ownership of the Service other than for training purposes or under the guidelines referred to previously.

9.1.4 Images retained for evidential purposes will be retained in a secure place where access is controlled.

9.2 Quality and Maintenance

In order to ensure that clear images are recorded at all times the equipment for making recordings and the associated security equipment will be maintained in good working order with regular servicing in accordance with the manufacturer's instructions. In the event of a malfunction the equipment will be repaired within specific time scales which will be scheduled within the maintenance agreement. All documentation relating to the equipment and its servicing and malfunction is retained in the control room and will be available for inspection and audit.

9.3 Media Log

A Media Log will be maintained at all times to document and track all material recorded and produced. The log shall record the following:

a) Unique reference number(s)
b) Time/date/person producing material for third party request
c) Time/date/person removing material from secure storage
d) Time/date/person returning material to secure storage
e) Additional comments (e.g. destruction, handed to law enforcement)

9.4 Making Recordings

Details of the recording procedures are contained in the Procedural Manual.

Recording mediums containing original incidents should not be replayed, unless absolutely essential, to avoid any accident, damage or erasure. If recorded images need to be reviewed the reasons and details of those present will be logged and the medium returned to secure storage, if appropriate.

9.5 Image Prints

Image prints will only be made when absolutely necessary. All video prints will remain the property of the service owner. The taking of image prints will be recorded in the Media Log located in the Control Centre.

10. Documentation

10.1 Log books must be sequential in order that pages or entries cannot be removed and full and accurate records kept.

10.2 Incident Log Book

An accurate log of operator working times will be maintained. Each operator will maintain a log of any event or occurrence including:

a) Change of operator identifying the operator on duty at that workstation and showing that:

1. That the correct time was being displayed
2. That the recording equipment appeared to be operating correctly

b) Incidents including details of time, date, location, nature, name of operator dealing and action taken

c) Routine camera patrols, whether taken manually or through the utilisation of pre-set times

d) Privacy zones, detailing where, for any reason, it is necessary to encroach on private areas that are not part of the contractual patrol

10.3 Administrative documents

The following documents and logs shall be maintained at all times:

a) Fault Log

b) Staff Rota

c) Media Log

d) Visitor Log Book

e) Maintenance Log

f) Incident Log Book

g) Equipment Inventory

Version Control

Version	Changes/Comments	Officer	Approved by	Date adopted
1.0	New Code of Practice to replace old 2009 version.	Grant White	GCLT	01/04/2016
1.1	DBS requirement updated to meet level required.	Grant White	CCTV Manager	15/04/2016
1.2	S6.6.2 - Staff training requirement updated to match legal requirement on SIA S1.6.7 - Use of deployable CCTV cameras added	Grant White	CCTV Manager	06/07/2017
1.3	DPA references updated to reflect GDPR.	Grant White		