Haydon Wick
Parish Council

CLOSED CIRCUIT TELEVISION (CCTV) POLICY 2021

Contents

1 - Introductions & Definitions 4

1.1 Introduction 4

1.2 Ownership 4

1.3 CCTV Operational Requirements 4

1.4 CCTV Policy Mission Statement 5

1.5 Definitions 5

1.6 System Description 6

2 Changes to the Code of Practice 6

2.1 Changes to the Code of Practice 6

2.2 Supplementary Documentation 7

3 Objectives of the CCTV Policy 7

3.1 Purpose of and Compliance with the CCTV Policy 7

3.2 Objectives of the CCTV System 7

4 Fundamental Principles & Policies 8

4.1 Rights of Privacy 8

4.2 Principles of Management 8

4.3 Signage 9

4.4 Point of Contact 9

4.5 Release of information to the Public 9

4.6 Release of information to statutory prosecuting bodies 10

4.7 Annual Policy Review 10

5 – Data Protection Act 2018 & Other Legislation 10

5.1 Information Commissioner's Office (ICO), Data Protection Act 2018 (DPA), General Data Protection Regulations (GDPR) 10

5.2 Human Rights Act 1998 11

5.3 Criminal Procedures and Investigations Act 1996 12

5.4 Freedom of Information Act 2000 12

5.5 Regulation of Investigatory Powers Act 2000 12

5.6 Surveillance Camera Code of Practice (Protection of Freedoms Act 2012) 13

5.7 Crime and Courts Act 2013 15

6 – Accountability 15

6.1 Support of Principles 15

6.2 Accountability 15

6.3 Annual Assessment 16

6.4 Complaints 16

6.6 Staff Training 16

7 – Control Room Management & Operation 17

7.1 Access to the Control Room 17
7.2 Response to Incidents 17
7.3 Observation & Recording Incidents 18
7.4 Successful Response 18
8 – Privacy & Disclosure Issues 18
8.1 Privacy 18
8.2 Disclosure Policy 18
8.3 Viewing of Recorded Images 19
8.4 Operator Competency 19
8.5 Subject Access Request 19
8.6 Other Rights 20
9 – Recorded Material Management 20
9.1 Recorded Material Management 20
9.2 Quality & Maintenance 21
9.3 Extraction of Recorded Images 21
9.4 Making Recordings 21
9.5 Copies of Recorded Images 21
10 – Documentation 22
10.1 Logs and Administrative Documents 22

1 - Introductions & Definitions

1.1 Introduction

This Policy shall apply to the Haydon Wick Parish Council (HWPC), Closed Circuit Television system ('the CCTV System'). The CCTV system comprises of a number of surveillance cameras in specific locations within the controlled areas within the HWPC boundary, with control, monitoring and recording facilities at a dedicated location. The operational requirement for the CCTV system has been assessed through review of historical events/incidents and concerns identified within the respective locations. The CCTV System has, therefore, been implemented to enable areas to be monitored and images captured and reviewed as required to support the observation of persons and detection of matters/incidents within the specified areas, as well as the identification and recognition of persons in accordance with the operational requirements. The primary use of the CCTV system will be to review new and existing footage, however, should the necessity arise, the facility to monitor live footage is also available.

1.2 Ownership

The CCTV System is owned by HWPC who are responsible for the management, administration, security and integrity of the system. As such, HWPC will ensure that all relevant legislation is adhered to in accordance with the Surveillance Camera Commissioner, and the Information Commissioner's Office (ICO).

1.3 CCTV Operational Requirements

The operational requirements for the CCTV system have been assessed through review of historical events and concerns within the relative locations.

The principles purposes of the CCTV system are as follows:

- To promote public confidence by developing a safe and secure environment.
- To ensure the safety of staff, leisure garden holders, visitors to the Parish and residents.
- To assist in the monitoring, identification, investigation, and enforcement of action whereby crime is suspected to have been committed through provision of footage as evidence, as applicable.
- To assist in the maintenance of public order and reduction of offences involving vandalism and antisocial behaviour.
- To provide assistance and reassurance to the public in the event of an emergency.

HWPC is committed to the recommendations contained within the Surveillance Camera Commissioner's Code of Practice and the ICOs guidance. These can be found at: www.gov.uk/government/organisations/surveillance-camera-commissioner and www.ico.gov.uk.

1.4 CCTV Policy Mission Statement

To inspire public confidence by ensuring that all public area CCTV systems, which are linked to the CCTV Control and Monitoring Room, are operated in a manner that always demonstrates integrity and preserve the civil liberty of law-abiding citizens.

1.5 Definitions

1.5.1 '**The CCTV System' –** The Closed Circuit Television System owned and implemented by HWPC, comprised of cameras and associated equipment for monitoring, transmission and processing purposes.

1.5.2 **The CCTV Control and Monitoring Room** – The secure area of a building whereby the monitoring and reviewing of CCTV footage, both live and recorded, can take place, and whereby the data can be retrieved, analysed and processed as appropriate.

1.5.3 **Data –** All information, including that about an individual, and any other associated linked or processed information.

1.5.4 **Personal Data –** Data which relates to an individual, who can be identified from that data, either with or without other data that is in the possession of, or accessible by, the data controller.

1.5.5 **Sensitive Personal Data -** Personal data which is deemed to be sensitive. The most significant of these, for the purposes of this code, are information about:

- The commission, or alleged commission, of any offences,
- Any proceedings for any offences committed, or alleged to have been committed, the disposal of such proceedings, or the sentence of any court in such proceedings.

1.5.6 **"Incident" –** An activity that raises cause for concern for the safety and/or security of an individual or property, inclusive of vehicle. This includes whereby an offence has been committed, is about to be committed, or any other occurrence that requires specific action to be taken by an operator.

1.5.7 **"Owner" –** The owner is HWPC, the organisation with overall responsibility for the formulation and implementation of policies, procedures, control and integrity of the system.

1.5.8 **Manager -** The manager of the system is the Chief Officer of HWPC, and has the responsibility for the implementation of and adherence to the policies, purposes and methods of control of a CCTV scheme, as defined by the owner.

1.5.9 **Data Controller –** The data controller for the CCTV system is the Deputy Clerk of HWPC and is responsible for determining the purposes for which, and the manner in which, any personal data is processed.

1.5.10 **"Operators" –** Employees of HWPC or contractors employed by the Council specifically designated to carry out the physical operation of controlling the CCTV system and the data generated. All operators are screened, trained and licensed to the standards required by the Private Security Industry Act 2001.

If contractors employed by the Council are reviewing the footage outside of the Control Room, then strict boundaries are set and stipulated within the procedural documents. A copy of the operators' CCTV licences and a register of authorised users will be regularly maintained for due diligence purposes.

1.5.11 **"Recorded footage" –** Any footage or images that have been recorded. Footage that is not live.

1.6 System Description

1.6.1 The CCTV system consists of fully functional cameras (pan, tilt and zoom (PTZ) capabilities), and a transmission system to enable images to be viewed at the HWPC CCTV Control and Monitoring room.

1.6.2 Images from all cameras are recorded based on motion detection, or manual activation, 24 hours a day, 365 days day of the year. The CCTV system is operational and is capable of being monitored throughout this period, should the necessity arise.

1.6.3 The physical and intellectual rights in relation to any and all material recorded within the Control and Monitoring facility shall, at all times, remain in the ownership of HWPC.

2 Changes to the Code of Practice

2.1 Changes to the Code of Practice

Any major changes to this policy will take place only after consultation with the relevant managerial personnel, and upon agreement by all organisations associated with the operation of the system.

2.1.1 **Major changes** to this policy are defined as changes that affect its fundamental principles and shall be deemed to include:

- additions and omissions of cameras to the system
- matters which have privacy implications
- additions to permitted usage criteria
- changes in the right of access to personal data, except statutory requirements - significant legal implications.

2.1.2 **Minor changes** to this policy are defined as operational and procedural matters which do not affect the fundamental principles and purposes; these include:

- additions and omissions of contractors
- additional clarifications, explanations and corrections to the existing code
- additions to the code of practice 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 the owner of the system.

The CCTV Policy will be subject to annual review, which will include compliance with the relevant legislations and standards.

2.2 Supplementary Documentation

This CCTV Policy will be supplemented by the following documents:

- HWPC Operational Procedures Manual

This document contains instruction and guidance for all those involved in the operation of the system to ensure that all principles within this policy are adhered to The Operational Procedures Manual will be a restricted document, available only to employees and relevant personnel.

3 Objectives of the CCTV Policy

3.1 Purpose of and Compliance with the CCTV Policy

3.1.1 This CCTV Policy is provided to detail the management, operation, administration and integrity of the CCTV system implemented within the Haydon Wick Parish, and the CCTV Control and Monitoring room.

3.1.2. This policy is in place both to assist all owners, managers, and operators to understand their legal and moral obligations and to reassure the public about the safeguards in place, as stated.

3.1.3. The owners, CCTV Operators and users of the CCTV systems and associated safety and security equipment connected to the Control, Monitoring and Recording facility shall be required to demonstrate formal agreement that they will comply with this policy and its contents).

3.1.4 All those entering the control room are bound by confidentiality, with visitors reading the confidentiality statement and signing the visitor log to confirm their understanding and acceptance that they will treat any viewed and/or written material as being strictly confidential. That they undertake to not divulge details of the images or information it to any other person/s or organisation/s. And the use of mobile phones or other recording devices will be strictly controlled in the CCTV control room?

3.2 Objectives of the CCTV System

The following objectives have been established CCTV system:

- Assisting in the maintenance of public order and reducing offences involving vandalism, nuisance, and antisocial behaviour

- The detection, prevention and mitigation of criminal activity and promoting a safe environment for the public within HWPC open spaces

- Providing evidence to support the apprehension and prosecution of offenders

- To deter individuals from damaging property or assist in identifying those who cause damage to property.

- Enabling assistance to be provided to and reassuring the public in emergency situations

4 Fundamental Principles & Policies

4.1 Rights of Privacy

HWPC support the individual's right to privacy and will insist that all agencies involved in the provision and use of the CCTV system accept this fundamental principle as being paramount.

4.2 Principles of Management

4.2.1. Prior to the installation of cameras, an 'Impact Assessment', to determine whether a camera is justified and how it will be operated, will be undertaken in compliance with the ICO's CCTV Code of Practice. This includes identification of the Operational Requirement for each proposed camera, in order to specify the quality of the images and functionality of cameras required. This is as recommended by the ICO.

4.2.2. That the cameras have been sited to capture images that are relevant to the specified purposes for which the system has been established.

4.2.3. Cameras will be sited to ensure that they can produce images of sufficient quality, ensuring consideration for technical and environmental issues.

4.2.4. To accomplish the above, an 'Operational Requirement' will be completed at the time of the 'Impact Assessment' for each proposed camera to dictate the quality of images required. This is a recommendation of the ICO.

4.2.5. Whereby wireless transmission systems are used to control CCTV equipment, sufficient safeguards will be in place to ensure the integrity of the data captured is maintained.

4.2.6. The CCTV system will be operated fairly, within the applicable laws, and only for the purposes for which it is established, or which are subsequently agreed in accordance with this CCTV Policy.

4.2.7. The system will only be operated by trained and authorised personnel. Operators will be aware of the legislation applicable to the operation of the CCTV system and the

handling of any associated data, as well as the purposes for which the CCTV system has been implemented. As a result, the CCTV system will only be used to achieve the identified purposes.

4.2.8. The CCTV system will be operated with due regard for the privacy of the individual/s.

4.3 Signage

The CCTV system has been implemented to provide surveillance of HWPC Open Spaces and controlled areas within the Parish, in order to fulfil the stated purposes of the CCTV system.

The area protected by CCTV will be indicated by the presence of signs. The signs will be placed sufficiently to ensure public awareness that an area is being monitored by CCTV.

The signs will state the organisation responsible for the scheme and the website address from which further information can be requested.

Data will not be held for longer than necessary and disposal of information will be regulated, in accordance with General Data Protection Regulations (GDPR).

4.4 Point of Contact

Should the public wish to contact the manager of the CCTV system, they may write to, or email

The CCTV Manager
Haydon Wick Parish Council
The Council Offices
Thames Avenue
Haydon Wick
Swindon
SN25 1QQ

clerk@haydonwick.gov.uk

4.5 Release of information to the Public

Information will be released to third parties, (see Section 8), who can demonstrate legitimate and reasonable grounds for the information to be released. Any request for the release of information must be made in writing with appropriate identification also being provided. Information will only be released if the request complies with current legislation and on the understanding that the information is not used for any other than that specifics in the written request.

Individuals may request to view information concerning themselves held on record in accordance with the Data Protection Act 2018 (DPA) and GDPR, through a Subject Access Request (SAR). The procedure is outlined in Section 8.9 of this policy.

4.6 Release of information to statutory prosecuting bodies

Information may be released to statutory prosecuting bodies, such as the Police, and statutory authorities with powers to prosecute and facilitate the legitimate use of the data derived from the CCTV system.

Statutory bodies may have access to data, including footage, if permitted for disclosure on application to the owner of the system, or the manager, provided the reasons and statement of purpose, are in accordance with the objectives of the CCTV system, and conditions outlined in Section 8 of this policy.

All data provided will be treated as evidential exhibits.

4.7 Annual Policy Review

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

- Any change to validity of operational requirement or objectives
- Changes to the CCTV System
- Review of the Data Protection Act 2018 and legislations associated to the usage of CCTV systems
- Maintenance log and any ongoing and outstanding issues
- Complaints Procedure
- Identification of trends

5 – Data Protection Act 2018 & Other Legislation

5.1 Information Commissioner's Office (ICO), Data Protection Act 2018 (DPA), General Data Protection Regulations (GDPR)

5.1.1 The CCTV System is registered with the ICO. Registration Number: Z7352658.

5.1.2 The CCTV System will be managed in accordance with the DPA 2018 and the Articles of the GDPR. Both Part 3 Chapter 2 of the DPA (processing personal data for law enforcement purposes) and Article 5 of the GDPR are comprised of six Data Protection Principles, a summary of which follows:

First Data Protection Principle;
Lawfulness, fairness and transparency.

- Processing of personal data for any of the law enforcement purposes must be lawful and fair.

Second Data Protection Principle;
‘Purpose Limitation’

- The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and;
- Personal data collected must not be processed in a manner that is incompatible with the purpose for which it was originally collected.

Third Data Protection Principle; ‘Data Minimisation’

- Personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

Fourth Data Protection Principle;
‘Accuracy’

- Personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and;
- Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

Fifth Data Protection Principle;
‘Storage Limitation’

- Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

Sixth Data Protection Principle;
‘Integrity and Confidentiality

- Personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security and integrity of the personal data, using appropriate technical or organisational measures (and, in this principle, ‘appropriate security’ includes protection against unauthorised, or unlawful processing and against accidental loss, destruction or damage).

5.2 Human Rights Act 1998

The CCTV System will be operated by, or on behalf of, a public authority. HWPC has considered the wider human rights issues, specifically 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) HWPC will always consider the following:

- Proportionality – 4.2.1., 4.2.2., 4.2.3., 4.2.4., 4.2.6.
- Legality - 4.2.6., 4.2.7., 4.2.8.
- Accountability – 4.2.7.
- Necessity/Compulsion – 4.2.3., 4.2.4.

Any infringement by a public authority of another's rights must be justified.

5.3 Criminal Procedures and Investigations Act 1996

The Criminal Procedure and Investigations Act 1996 (CPIA) concerns the disclosure of what has been seized under powers and places a duty on the police, or other investigating personnel, to pursue all reasonable lines of enquiry to obtain relevant evidence.

The impact on the CCTV operator is that there may be a request to access a large amount footage including images not of a particular incident, but from adjacent cameras. This would be for the purpose of confirming that an activity was, or was not, carried out by an individual, or similar.

The police may also wish to retain written notes and logs if they deem them to be appropriate and in support of their investigation. It is the responsibility of the police (or other agency) to adhere to the 'disclosure' process in respect of any legal defence, not the CCTV operator, whose role will be to provide that evidence to the police, or other agency. Disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on the data controller by the DPA 2018 and the GDPR (known as subject access).

5.4 Freedom of Information Act 2000

If a request for images is received via a Freedom of Information Act (FOIA) application and the person requesting is the subject, these will be exempt from the FOIA and will be dealt with under the DPA2018 and GDPR (Subject Access Request, 8.6).

Any other requests not involving identification of individuals can be disclosed but only if it does not breach the DPA 2018 and GDPR.

5.5 Regulation of Investigatory Powers Act 2000

Introduction

The Regulation of Investigatory Powers Act (RIPA) 2000 came into effect on 2 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' are part of the duties of many law enforcement officers and other public bodies. An example of this would be where police officers are seen at locations monitoring crowds to maintain public safety and prevent disorder. Officers may also target a crime 'hot spot in order to identify and potentially arrest suspected 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 the 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 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 RIPA.

The provisions of the Act do not 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. It was not envisaged that this Act would have significant impact on specific, targeted use of public/private CCTV systems by 'relevant Public Authorities' covered in Schedule 1: Part 1 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. (PACE)

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.

Any HWPC CCTV System will observe the criteria laid out in the legislative requirements. Further information is available from the Home Office website.

5.6 Surveillance Camera Code of Practice (Protection of Freedoms Act 2012)

The Surveillance Camera Code of Practice was required in conjunction with the Protection of Freedoms Act 2012 to determine guidelines for CCTV systems to ensure that the usage of such is open and proportionate, as well as to ensure that the quality of images captured enhance the opportunity for identification of those who have committed offences.

This code of practice encompasses 12 guiding principles, providing a framework of good practice, inclusive of existing legal obligations. Such legal obligations include processing of data under the DPA 2018, the Human Rights Act 1998, and RIPA 2000.

The 12 guiding principles are as follows:

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.

2. The use of a surveillance camera system must take into account its effect/impact on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be appropriate transparency in the use of a surveillance camera system, including a published contact point for access to information and complaints.

4. There must be clear responsibility, segregation of duties and accountability for all surveillance camera system activities, including the collection/storage of images and information, held and used.

5. Clear criteria, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. Images and information should be stored and managed with GDPR requirements and that which is required for the stated purpose of a surveillance camera system.

7. Access to retained images and information should be restricted and there must be clearly defined criteria as to who , when and for what purpose the data can be accessed the disclosure of images and information should only take place when it is necessary for such a purpose, or at the request of law enforcement agencies..

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be an effective review and audit mechanisms in place to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be available and published.

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.

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.

Whilst adherence to these principles is voluntary, HWPC will ensure that continued compliance is maintained. Information and a copy of this code of practice can be found via www.gov.uk.

5.7 Crime and Courts Act 2013

The Crime and Courts Act became law on 1 October 2013 and replaced the Serious Organised Crime and Police Act 2005. CCTV Control Rooms 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 HWPC I CCTV Control room 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 SAR) – which help financial institutions protect themselves, their customers and their reputation from financial crime 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.

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

HWPC 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 HWPC to maintain a continuous review of its CCTV systems integrity, security, procedural efficiency, methods of operation and retention and release of data. The 'Single Point of Contact' for HWPC with regards to the CCTV system and operations is the CCTV Manager.

6.2 Accountability

6.2.1 The **CCTV Manager** is accountable to the CCTV owner, and will resolve technical and operational matters where possible. The CCTV manager is responsible for ensuring that staff/authorised personnel are appropriately trained, that this training is documented and certified by the Security Industry Authority (SIA) and all policies, procedures and its integrity are adhered to upheld with regards to the CCTV system.

6.2.2 The **Data Controller** is responsible for the security, storage and integrity of data, the releasing of data to third parties who have legal right to receive copies of such.

6.2.3 All **Operators** are responsible for complying with this policy and all other associated policies and procedures. The operator has a responsibility to understand and comply with the objectives of the CCTV system, and respect the privacy of the individual whilst doing so.

All operators are required to be proficient in the control and the use of the CCTV camera equipment, recording and playback facilities, media procedures and maintenance of all logs. The information recorded must be accurate, adequate and relevant to the purpose of the CCTV system.

Should any faults be identified by the Operator, it is the Operators responsibility to report these to the appropriate person(s) at the earliest practicable opportunity.

Failure of the operators to comply with the procedures and code of practice should be dealt with by the manager. Person(s) misusing the system will be subject to disciplinary or legal proceedings in accordance with the employer's policy.

6.3 Annual Assessment

An annual assessment of the scheme will be undertaken by an independent consultant appointed by the owner to evaluate the effectiveness of the system. This will include annual reviews of the scheme's operation, performance and working practices and, where appropriate make recommendations for improvements.

The results will be assessed against the stated purposes of the scheme. If the scheme is not achieving its purpose modification and other options will be considered.

The results of the assessment will be made available through HWPC.

The ICO's CCTV Code of Practice stipulates that the system should be reviewed annually to determine whether CCTV continues to be justified. It further states that it is necessary to establish the system's effectiveness to ensure that it is continuing to meet the operational requirement. If it does not achieve the purpose for which it was intended, it should be stopped or modified.

6.4 Complaints

A member of the public wishing to make a complaint about the system may do so through HWPC complaints procedure. A copy of this procedure can be found via: www.haydonwick.gov.uk.

A record of the number of complaints and nature, or enquiries received will be maintained together the action taken.

6.6 Staff Training

All operators are, or will be, trained to the criteria required by the Private Security Industry Act 2001 and licensed by the SIA for use of Public Space Surveillance (CCTV).

All persons employed to act as operators of the system will be trained to the highest available standard and documented. Training will be completed by suitably qualified persons and will include:

- The Roles and Responsibilities of CCTV Operators
- The Characteristics and Equipment of a CCTV System
- Relevant Legislation
- ICO's Code of Practice for CCTV systems
- All policies and procedures regarding CCTV systems
- Terms of employment
- The use of all appropriate equipment
- The operation of the systems in place
- The management of recorded material including requirements for handling and storage of material needed for evidential purposes
- All relevant legal issues including Data Protection Act 2018 and Human Rights Act 1998

7 – Control Room Management & Operation

7.1 Access to the Control Room

7.1.1 At any time whereby the review or monitoring of CCTV footage, live or recorded, is carried out, the Control Room is to be a secure environment. To ensure this, the access point to this room will be locked, with only authorised personnel with a legitimate purpose permitted access.

All visitors to the CCTV control room including Police Officers, will be required to sign in as visitors to declare attendance and compliance with the confidentiality statement and requirements.

7.1.2 The Manager/Data Controller is authorised to determine who has access to the monitoring area.

This will normally be:

- Operating staff/authorised personnel
- The Manager/Supervisor
- Police officers requiring to view images, or collecting/returning media being considered for intelligence or evidential purposes
- Engineers (with supervision throughout their visit)
- Independent consultants appointed for system audit purposes

7.2 Response to Incidents

7.2.1 The primary function of the HWPC CCTV System is for review of recorded footage, as opposed to monitoring of live footage. Should the necessity arise, the capability to monitor live footage is available. Should the CCTV Control Room be notified of an incident within an area covered by the CCTV system, live monitoring will take place if

reasonably practicable. The CCTV Control Room is manned between the hours of 09:00 – 15.30.

7.2.2 Incidents of a criminal nature will be reported to Wiltshire Police, who will respond in accordance with their policies and procedures.

7.2.3 A record of all incidents will be maintained in the incident log. This log will detail anything that may contribute to investigational proceedings or evidential purposes.

7.3 Observation & Recording Incidents

The CCTV system will record when motion is detected within the parameters of the camera, or on manual request,24 hours a day, 365 days a year. In the event of an incident being identified during Control Room operating hours, there will be a particular focus on the relevant area.

7.4 Successful Response

The criteria for a successful response is:

- A good observational record of the incident
- Identification of a suspect
- The prevention or minimisation of injury or damage
- Reduction of crime and disorder
- Improving public safety

8 – Privacy & Disclosure Issues

8.1 Privacy

Cameras will not be used to infringe the individual's rights of privacy. Whereby cameras are sited with a potential view of residential properties that would intrude in private areas, physical screening will be implemented, or the appropriate privacy zones will be programmed into the cameras where possible, and CCTV operators trained to recognise privacy issues.

8.2 Disclosure Policy

The following principles must be adhered to:

1. All employees will be aware of the restrictions stated within this policy with regards to access to, and disclosure of, recorded images.

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

3. Recorded material will only be used for the purposes defined in the objectives and policy.

4. Information will not be disclosed for commercial purposes and entertainment purposes.

5. All access to the medium on which the images are recorded will be documented.

6. Access to recorded images will be by authorised personnel with a legitimate purpose only.

7. Viewing of the recorded images will take place in a restricted area.

8.3 Viewing of Recorded Images

At any time whereby the review or monitoring of CCTV footage is carried out, the Control Room is to be a secure environment. To ensure this, the access point to this room will be locked, with only authorised personnel with a legitimate purpose permitted access.

8.4 Operator Competency

All Operators are required to have an appropriate understanding of the privacy and disclosure issues relating to the CCTV system.

8.5 Subject Access Request

8.5.1 All staff/authorised personnel involved in operating the equipment must be able to recognise a request, both verbal and written, for access to recorded images by data subjects, and be aware of individual's rights under this section of the Code of Practice.

8.5.2 Individuals whose images are recorded have a right to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images. This must be provided within one month of receiving a request.

The individual will be required to provide identification in order to validate the request.

8.5.3 An extension of the one-month time period may be extended by up to a further two months, if the request is complex, or multiple requests have been made by the subject. Should the necessity to extend the time frame within which data will be provided, the individual must be contacted within one month of receiving the request to explain why the extension is necessary.

8.5.4 Whereby a verbal request is made, the employee to whom it was directed must document the request.

8.5.5 If images of third parties are also shown with the images of the person who has made the access request, consideration will be given as to whether there is a need to obscure the images of third parties. If providing these images would involve an unfair intrusion into the privacy of the third party, or cause unwarranted harm or distress, then they should be obscured. Alternatively, a written documentation may be provided if the obscuring of the third party is not practicable.

8.5.6 A search request should provide sufficient information to locate the data requested (e.g.

within 30 minutes for a given date and location). If insufficient information is provided a data controller may refuse a request until further clarification is received

8.5.7 A reasonable administrative fee may be applicable for any request, in accordance with GDPR.

8.5.8 Refusal of provision of data in response to a SAR will be fully documented if applicable.

Further information with regards to requesting data via Subject Access Request can be found via:
www. ico.org.uk/your-data-matters/your-right-to-get-copies-of-your-data

8.6 Other Rights

8.6.1 All staff/authorised personnel 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.

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

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

8.6.4 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.

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

9 Recorded Material Management

9.1 Recorded Material Management

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. Footage will be stored on the CCTV system for a period of 30 days only. Recorded images may need to be extracted and retained for longer periods as a requirement of an investigation into crime. Whilst images are retained, access to and security of the images will be controlled in accordance with the requirements of the Data Protection Act 2018.

9.1.1 Recorded material should be of high quality. In order for recorded material to be admissible in court, total integrity and continuity of evidence 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 images will not be released to organisations outside the ownership of the system other than as previously stated.

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

9.2 Quality & Maintenance

In order to ensure that full functionality of the CCTV system is maintained, a functional check on each of the cameras, and the recording system, will be carried out on a weekly basis. Detail of any maintenance action to be taken will be documented, and actions passed to the relevant persons and/or departments to be resolved at the earliest opportunity.

9.3 Extraction of Recorded Images

Full documentation of all extractions of recorded images, and actions taken with such, will be fully documented whilst in the possession of HWPC.

This documentation will include the following:

- Unique equipment reference number(s)
- Time/date/person extracting the footage
- Time/date/person removing/returning footage to the secure storage
- Time and date of delivery to the law enforcement agencies
- Enforcement agency officer concerned
- Details of all reviews of images, including persons present

Recorded material will be securely stored. Data to be destroyed will be destroyed as a controlled operation, with full documentation.

Special consideration will be given to recorded material that has been requested by the Police or contains a known incident. This is elaborated within the Operational Procedures Manual.

9.4 Making Recordings

Details of the recording procedures are given in the Operational Procedures Manual.

Recordings 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 recordings returned to secure storage, if appropriate.

9.5 Copies of Recorded Images

Copies of Recorded Images will only be made when absolutely necessary. All copies will remain the property of the system owner. The removal of copies will be recorded in a register to be retained in the control room.

10 – Documentation

10.1 Logs and Administrative Documents

The following documents shall be maintained:

- System Access Log
- Activity Log
- Incident Reports
- Visitor Log
- Functional Check Log
- Evidence Log
- Destruction of Recordings Log
- System Specification Technical Site Assessment

Version control

2020 HWPC CCTV Policy	Georgina Morgan-Denn Clerk to Council	Adopted at Full Council 25th February 2020 FC 198 B	Review: when required
2021 Revision to 1.5.10 Contractors	Georgina Morgan-Denn Chief Officer	Adopted at Finance & Policy Committee 17th August 2021 FC Minute Reference here	