whg

CODE OF PRACTICE

For

CCTV and Body Worn Video

CONTENTS

1.0 INTRODUCTIONS AND DEFINITIONS

1.0 Introduction

This Code of Practice shall apply to the closed-circuit television surveillance scheme known as the whg CCTV scheme. The scheme initially comprises of cameras located in specific external and internal locations within the whg area, with control, monitoring and recording facilities at a dedicated location. A problem orientated process was utilised to assess the requirements of the CCTV cameras within individual locations. The cameras have therefore been sited to capture images which are relevant to the purposes for which the schemes have been established.

1.1 Ownership

The system is owned by Walsall Housing Group Limited (whg) who is responsible for the management, administration and security of the systems. whg will therefore ensure the protection of individuals and the public by complying with the Biometrics and Surveillance Camera Commissioner 'Surveillance Camera Code of Practice' and the Information Commissioner's CCTV Code of Practice and this document.

1.2 Closed Circuit Television Mission Statement

To promote public confidence by developing a safe and secure environment for the benefit of those visiting, employed or residing in the area covered by whg CCTV system. whg is committed to the recommendations contained in the Biometrics and Surveillance Camera Commissioner 'Surveillance Camera Code of Practice' and the Information Commissioner's CCTV Code of Practice which can be found on the following websites: www.gov.uk and www.ico.gov.uk.

1.3 Codes of Practice Mission Statement

To inspire public confidence by ensuring that all public area Closed Circuit Television (CCTV) systems which are linked to the CCTV Control and Monitoring Room are operated in a manner that will secure their consistent effectiveness and preserve the civil liberty of law-abiding citizens at all times.

1.4 Definitions

The CCTV control and monitoring room shall mean the secure area of a building where CCTV is monitored and where data is retrieved, analysed and processed.

CCTV scheme shall mean the totality of the arrangements for closed circuit television in the locality and is not limited to the technological system, staff and operational procedures.

The retrieval system means the capability, in any medium, of effectively capturing data that can be retrieved, viewed or processed.

Processing means obtaining, processing, recording or holding the information or data or carrying out any operation or set of operations on the information or data. The full definition is explained in the Data Protection Act 2018.

CCTV system means the surveillance items comprising cameras and associated equipment for monitoring, recording, transmission and controlling purposes, for use in a defined zone.

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

Personal Data means data which relates to a living individual who can be identified: a) from that data or 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.

Sensitive personal data is 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 offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

An incident is an activity that raises cause for concern that the safety or security of an individual may 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.

The owner is whg and is the organisation with overall responsibility for the formulation and implementation of policies, purposes and control of the scheme.

The system manager (Community Safety Manager) has the responsibility for the implementation of the policies, purposes and methods of control of a CCTV scheme, as defined by the owner of the scheme.

Data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are about to be processed. The Data Controller in the case is of the CCTV systems referred to in this Code of Practice is whg.

Operators are either employees of whg or third-party contract staff who are 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 in the Private Security Industry Act 2001.

Recording material means any medium that has the capacity to store data and from which data can later be recalled irrespective of time.

1.5 System description

The Closed Circuit Television systems referred to in this document have been introduced into the premises for the purposes outlined in Section two. Whilst the scheme is owned by whg its implementation and/or expansion is supported by the following bodies (the partners)

- West Midlands Police
- Safety Forums
- Residents and employees

The owner, and all partners will work in accordance with the Codes. The partners will have no involvement in the operating of the system with the exception of the Police.

Images from all cameras are recorded simultaneously throughout 24-hour period 365 days each year.

The system is capable of being actively monitored by the police or authorised trained personnel according to operational needs.

High quality cameras are in use. The physical and intellectual rights in relation to any and all material recorded by the systems shall at all times remain in the ownership of whg.

2.0 PURPOSES OF THE CODE OF PRACTICE AND CCTV SCHEME

2.1 Consultation

Any major changes to this Code of Practice will take place only after consultation with the relevant management group.

Major changes to this code 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 uses criteria e.g. purposes of the scheme
- changes in the right of access to personal data, except statutory requirements
- significant legal implications.

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:

- 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 Code of Practice will be subject to annual review which will include compliance with the relevant legislation and Standards.

2.2 Supplementary Documentation

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

- CCTV Operations Procedural Manual
- Manufacturers Equipment manual

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

3.0 OBJECTIVES OF THE CCTV SCHEME & CODE OF PRACTICE

3.1 Purpose of and Compliance with the Code of Practice

This Code of Practice is to detail the management, administration and operation of the closed circuit television (CCTV) system in the specified areas and the associated Control, Monitoring and Recording Facilities.

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

The owners and users of the CCTV system 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.

The owners, users and any visitors to the Control, Monitoring and Recording facilities 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 Purposes of the scheme

The following are the objectives for which the CCTV systems were established:

a) reducing the fear of crime

b) deterring and preventing crime

c) assisting in the maintenance of public order and reducing offences involving vandalism and nuisance

d) providing evidence which may assist in the detection of crime and the apprehension and prosecution of offenders

e) protecting property

f) providing assistance with civil claims

g) providing assistance with issues relating to public safety and health

h) providing assistance and reassurance to the public in emergency situations

i) providing reassurance to those who reside, work or visit the area of coverage

4.0 FUNDAMENTAL PRINCIPLES

4.1 Rights of Privacy

whg and partners support the individual's right to privacy and will insist that all agencies involved in the provision and use of Public CCTV systems owned by the organisation accept this fundamental principle as being paramount.

4.2 Principles of management of the scheme

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 Biometrics and Surveillance Camera Commissioner 'Surveillance Camera Code of Practice' and the Information Commissioner's CCTV Code of Practice.

The cameras have been sited to capture images that are relevant to the purpose for which the scheme has been established. Cameras will be sited to ensure that they can produce images of the right quality, taking into account technical and environmental issues

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 Biometrics and Surveillance Camera Commissioner.

The scheme 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 the Code of Practice.

Those who have authorised access are aware of the purpose(s) for which the scheme has been established and that the CCTV equipment is only used to achieve the identified purposes.

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

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

The need for formal authorisation to conduct covert 'Directed' surveillance as required by the Regulations of Investigatory Powers Act 2016 will be complied with.

The system will only be operated by trained and authorised personnel.

4.3 Policy of the Scheme and Signage

The scheme aims to provide surveillance of the public areas within the specified location, in order to fulfill the purposes of the scheme. 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 entering a zone which is covered by surveillance equipment.

The signs will state the organization responsible for the scheme, the purposes of the scheme 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 scheme they may write to:

whg
100 Hatherton Street
Walsall
WS1 1AB

The contact point will be available to members of the public during office hours. Enquiries will be provided with relevant documentation.

4.5 Release of information to the public

Information will be released to third parties who can show legitimate reasons for access. They will be required to request any information with reasons in writing and identify themselves. Information will be released if 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 the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). Information on how to obtain an application form can be obtained by writing to the above address.

4.6 Release of information to statutory prosecuting bodies

The policy is to assist statutory prosecuting bodies such as the Police, and statutory authorities with powers to prosecute and facilitate the legitimate use of the information derived from the scheme. Statutory bodies may have access to information permitted for disclosure on application to the owner of the scheme or the manager, provided the reasons and statement of purpose, accord with the objectives of the scheme and conditions outlined in section 7.3. 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 scheme
c) contracts with suppliers
d) a review of the data protection or legal requirements
e) maintenance schedule and performance test of the system
f) scheme evaluation findings
g) complaints procedure and evaluation

5.0 DATA PROTECTION ACT, OTHER LEGISLATION AND RECOMMENDATIONS

5.1 Data Protection Registration

The scheme is registered with the Data Protection Commissioner, Registration Number: Z667510X. The scheme will be managed in accordance with the principles of the Data Protection Act 2018 and the Articles of the General Data Protection Regulation.

5.2 Human Rights Act 1998

Where the system is 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). whg is not a public authority but acts within the spirit of the Human Rights Act 1998.

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) whg will always consider the following:

   - Proportionality - Article 4.2.1, 4.2.2, 4.2.3 and 4.2.6 of the code of practice
   - Legality - Article 4.2.7 and 4.2.8 of the code of practice
   - Accountability - Article 4.2.10 and 4.2.11 of the code of practice
   - Necessity/Compulsion - Article 4.2.3 of the code of practice

   Any infringement by a public authority of another's rights must be justified. If this is not the case then it will not be appropriate to use CCTV.

5.3 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 Data Protection Act 2018 and the General Data Protection Regulation (known as subject access).

5.4 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 Act 2018 and the GDPR.

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

5.5 Regulation of Investigatory Powers Act 2016

Introduction
The Regulation of Investigatory Powers Act 2016 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. whg is not a public authority.

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 2016 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.

Any whg CCTV scheme will observe the criteria laid out in the legislative requirements. Further information is available from the Home Office website:- www.homeoffice.gov.uk

5.6 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 2018 and the GDPR, 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.

Whilst the above principles are voluntary, Local Authorities must have regard to them and other organizations are encouraged to adopt the principles. whg is committed to achieve continued compliance with the requirements. Information and a copy of the Codes can be found on www.gov.uk.

6.0 ACCOUNTABILITY

6.1 Accountability

whg and its 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. The Single Point of Contact for whg is the Community Safety Manager (CCTV).

6.2 Hierarchy of Responsibilities

The Owner

The owner shall be responsible for policy, effective management and public relations of the scheme. They shall produce a written policy and be responsible for its implementation. This shall be carried out in consultation with users of the scheme 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 control and monitoring environment. The role of owner also includes all statutory responsibilities including the role of "data controller" as prescribed by the Data Protection Act 2018 and the GDPR.

The Manager

As the person with direct control of the CCTV scheme, the manager or other authorised person is responsible to the owner and should have authority for the following:

a) staff management (if appropriate);
b) observance of the policy and procedural practices;
c) release of data to third parties who have a legal right to copies;
d) control and security clearance of visitors;
e) security and storage of data;
f) security clearance of persons who request to view data;
g) release of new, and destruction of old, data and data medium;
h) liaison with the law enforcement agencies and other agencies;
i) maintenance of the quality of the recording and monitoring equipment; and
j) responsibility for maintenance of discipline on a day-to-day basis.

The manager should retain responsibility for the implementation of procedures to ensure that the CCTV system operates according to the objectives for which it was installed and in accordance with the objectives identified for the CCTV scheme.

The manager is responsible for the day-to-day liaison with all partners in, and users of, the CCTV scheme; this should include supervision of access to any data obtained by the CCTV scheme.

The manager should have responsibility for the instigation of disciplinary procedures against operators in matters relating to non-compliance with this British Standard, operational procedures and breaches of confidentiality or the unauthorized release of data.

The Supervisor (Operational Support)

The supervisor has a responsibility to ensure that at all times the system is operated in accordance with the policy and all procedural instructions relating to the system, and for bringing to the immediate attention of the manager any matter affecting the operation of the system, including any breach or suspected breach of the policy, procedural instructions, security of data or confidentially.

In the Manager's absence the Supervisor will have responsibility for all the duties of the manager as stated above.

- 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 scheme. This will include regular checks and audit trails to ensure that the documentation systems in place are working effectively. These systems include:

- The video image log
- The operators log
- The incident log
- Witness statements
- Faults and maintenance log
- The security of data
- Audit logs
- Authorisation of visitors – to be checked & counter signed by the Supervisor

The supervisor will ensure operators comply with Health and Safety Regulations.

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 scheme.

They are required to be proficient in the control and the use of the CCTV camera equipment, recording and playback facilities, image erasure, and maintenance of all logs. The information recorded must be accurate, adequate and relevant to the purpose of the scheme. They should bring to the attention of the supervisor immediately any equipment defect that may occur.

In the Manager's/Supervisor's absence the Operator will have responsibility for:

- 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

6.3 Accountability

The manager/supervisor shall be accountable to the owner of the scheme and will provide periodic progress reports on the scheme. The manager/supervisor will resolve technical and operational matters.

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

6.4 Annual Report

An annual report will be prepared for CCTV schemes monitoring public spaces. This report should be made available to the public.

The report will include the following details:

a) a description of the scheme and the geographical area(s) of operation;
b) the scheme's policy statement;
c) the objective and scope of the scheme;
d) any changes to the operation or management of the CCTV scheme;
e) any changes that have been made to the policy;
f) any proposals to expand or reduce the operation of the scheme; and
g) the scheme's aims and objectives for the next 12 months.

The report should also provide details of the scheme's achievements during the previous 12 months, which might be based on information already held by the scheme. The details of the scheme's performance should include:

1) the number of incidents recorded by the scheme;
2) the number of incidents reported to the law enforcement agencies and, where appropriate, other bodies, e.g. the local authority;

3) an assessment of the scheme's impact on crime levels and types of crime in the area covered by it; and
4) an assessment of the scheme's impact on its objectives, including:
    - the number of privacy impact assessments completed;
    - the number of reviews of footage by police and authorized agencies; and
    - the number of incidents per camera for the previous twelve months.

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 Biometrics and Surveillance Camera Commissioner 'Surveillance Camera 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 still doing what it was intended to do. If is does not achieve its purpose, it should be stopped or modified. British Standard 7958 for the Management and Operation of CCTV in public space also requires that an annual evaluation is undertaken.

6.5 Audit

Where schemes operate within the public domain, an independent audit should be conducted before the publication of the annual report. This audit should include the following:

a) the level of attainment of objectives and procedures;
b) random audits of all logs and the release of information;
c) the review policy; and
d) standard costs for the release or viewing of material.

The complaints procedure should be reviewed, with the following details included:

1) the number of complaints received;
2) the time taken to acknowledge and respond to complaints;
3) the method of receiving and handling complaints; and
4) the degree of customer satisfaction in handling complaints.

6.6 Complaints

A member of the public wishing to make a complaint about the system may do so through whg's complaint procedure. A copy of the complaints procedure is available by writing to:

whg
100 Hatherton Street
Walsall
WS1 1ST

A complaints procedure has been documented. A record of the number of complaints or enquiries received will be maintained together with an outline of the action taken.

When a complaint is received a written acknowledgement will be sent within three working days. A copy of the completed complaint form will also be sent so the complainant can check that the details are correct.

An investigation will follow and a written answer will be sent to the complainant within ten working days stating that:-

the investigation is complete giving details of any proposed action, or, the investigation has not been completed giving the reason why and a date when a full reply can be expected.

Should a complainant not be satisfied there is an appeals procedure and this is detailed in the full complaints procedure.

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

6.7 Personnel

Security screening

All personnel employed to control/operate or manage the scheme will be security screened in accordance with British Standard 7858: *Code of practice for screening of personnel in a security environment.*

Training

All 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 persons employed to act as operators of the system are trained to the highest available industry standard. Training has been completed by suitably qualified persons and has included:

- 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 and Human Rights
- Progression to nationally recognized qualifications
- Recognise and understanding privacy and disclosure issues
- The disciplinary policy

Contractors

There are special conditions imposed upon contractors carrying out works on the system. These are detailed within the contract with the contractor. It should be noted that wherever possible contractors should not have sight of any recorded data.

7.0 CCTV CONTROL FACILITY MANAGEMENT AND OPERATION

7.1 General

Access to the monitoring and recording areas will be strictly controlled.

Only those persons with a legitimate purpose will be permitted access to the Control, Recording and Monitoring Facility.

The CCTV System Manager or designated member of staff, is authorised to determine who has access to the monitoring area. This will normally be:

- Authorised Personnel/Operators (including authorised whg Representatives).
- Police officers requiring to view a particular incident, or intelligence or for evidential purposes. These visits will take place by prior appointment.
- Engineers and cleaning staff (These people will receive supervision throughout their visit).
- Independent Inspectors appointed under this Code of Practice may visit the monitoring and recording facility without prior appointment.
- Organised visits by authorised persons in controlled circumstances

All visitors to the monitoring and recording area, including Police Officers, will be required to sign a visitor's log and a declaration of confidentiality.

7.2 Response to an incident

The Procedural Manual details:

- What action should be taken
- Who should respond
- The time scale for response
- The times at which the observation should take place

A record of all incidents will be maintained in the incident log (this includes computerised systems. 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 West Midlands Police. 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 real time. Wherever possible the system 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

The criteria for measuring a successful response are:

- A good observational record of the incident
- A short time scale for response to the incident
- Identification of a suspect
- The prevention or minimisation of injury or damage
- Reduction of crime and disorder
- Improving public safety
- Restoration of tranquillity

7.6 Operation of the System by the Police

a) In the event of the police requesting use of the equipment from within the CCTV control room to monitor situations, such a request will only be permitted on the request of a Superintendent or his designated deputy and only with the permission of the System manager or his designated deputy. The request should be in writing, (email is acceptable), however, in emergencies this can be a verbal request which should then be followed by the written request as soon as practicable. The monitoring room will continue to be staffed and equipment operated by, only those personnel who are authorised to do so and who fall within the terms of this Code.

b) 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 monitoring room 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 and the Articles of the General Data Protection Regulation.

7.7 Body Worn Videos

The use of BWV is intended for “overt use” only and as such, they are not to be worn or used in a hidden or covert manner.

The Data Protection Act 2018 and the General Data Protection Regulation (GDPR) require that the data subject must be informed of:

- The identity of the Data Controller – which is Walsall Housing Group.
- The purpose or purposes for which the footage is intended to be processed.
- Any further information that is necessary for processing to be fair.

If possible, this information should be provided at the time they are being recorded or if this is not practicable due to an on-going incident then as soon as possible afterwards. The officer’s device shows that CCTV Recording is in progress.

Members of the public may be unaware that the camera is capable of recording sound. Officers should therefore, consider the reasonable expectations of the public (e.g. if a member of the public approaches them to ask a question they may not expect to be recorded and it is good practice for the officer to inform them that the device is switched on.

Recorded footage that is initially considered to be “non-evidential” should not be retained beyond the time where it is reasonably expected that it may be identified as being used for an investigation. Home Office guidance indicates that footage be retained for a period of 30 days for any investigation to become apparent after which it should be deleted.

More information on the use of Body Worn Videos can be obtained from whg.

8.0 PRIVACY AND DISCLOSURE ISSUES

8.1 Privacy

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

8.2 Disclosure Policy

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 scheme 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 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 system.
d) Monitors displaying images from areas in which individuals would have an expectation of privacy will not be viewed by anyone other than authorised persons.
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, where possible take place in a restricted area.

Before data is viewed by a third party the CCTV System Manager or designated member of staff 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 are maintained throughout
c) Not part of a current criminal investigation by the 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 authorised members 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

Where possible, the 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, in addition to being licensed as previously mentioned.

8.6 Removal of medium for Viewing

The removal of medium on which images are recorded, for viewing purposes, will be documented in accordance with Data Protection Act 2018, the Articles of GDPR and the procedural manual.

8.7 Access to data by third parties

Access to images by third parties will only be allowed in limited and prescribed circumstances. 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 the criminal enquiries or criminal proceedings.

All requests for access or for disclosure will be recorded. If access or disclosure is denied, the reason should be documented. If access to or disclosure of the images is allowed, details will be documented.

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.

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

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

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

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 individuals' rights under this section of the Code of Practice.

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 calendar month of receiving a request.

Data subjects requesting access will be provided with a standard subject Access request form (Appendix 'A') and accompanied leaflet (Appendix 'B') describing the types of images recorded and retained and the purposes for recording and retention. Subject access rights are governed by Data Protection Act 2018 and the General Data Protection Regulation and include the following provisions:

a) a person gives sufficient and accurate information about a date, 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

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 as been no captured images of identifiable individuals or information relating to individuals then this may not fall within the Data Protection Act 2018 and access may be denied. Any refusal should be documented.

If on the other hand images have been obtained 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 DPA and reference should be made to Section 8.2.2 of these Codes of Practice prior to the release of such data.

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 providing these images would involve an unfair intrusion into the privacy of the third party, or cause unwarranted harm or distress. whg's CCTV system does not currently have the capability of disguising or blurring the images of third parties. However, in many cases, images can be disclosed as there will not be an intrusion.

The subject access request will be dealt with promptly and in any case within one calendar month of receipt of the request or within a calendar month of receiving all the information required. All subject access requests should be dealt with by the manager or designated member of staff.

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.

Under certain circumstances (as defined with the Data Protection Act 2018 and the General Data Protection Regulation) 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 owner/manager having verified the validity of a request should provide requested material to the individual. If the individual agrees it may be possible to provide subject access by viewing only. If this is the case:

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

8.11 Other rights

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. 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.

The member 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. If the manager or designated member of staff decides that the request will not be complied with, they must set out their reasons in the response to the individual. A copy of the request and response will be retained.

8.12 Media Disclosure

Disclosure of images from the CCTV system must be controlled and consistent with the purpose for which the system was established. For example, if the system 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.

9.0 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 Data Protection Act and the General Data Protection Regulation.

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.

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

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

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 any 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 Digital Recordings

In a digital CCTV system, where possible, the register should show the life of the recorded media at all stages whilst in the owner's possession. Such a register may also show itself to be useful in enabling evaluation of the CCTV scheme. The register should include the following:

1) unique equipment reference number(s);
2) time/date/person removing medium from secure storage for use;
3) time/date/person returning medium to secure storage after use;
4) remarks column to cover additional points (e.g., erase/destroy/handed over to law enforcement agencies/removed from recording machine);
5) time and date of delivery to the law enforcement agencies, identifying the law enforcement agency officer concerned;

6) in the event of a non-automated system of erasure of data, the time/ date/ person responsible for erasure and/or destruction;
7) details of all reviews of images, including persons present and results.

9.4 Making Recordings

Details of the recording procedures are given 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 Video Prints

Video prints will only be made when absolutely necessary. Video Prints requested by police must be on written authority of an officer of the rank of Inspector or above. All video prints will remain the property of the scheme owner and those not handed to the police will be retained in a secure cabinet until destruction is authorised. The taking of video prints will be recorded in a register to be retained in the control room.

10.0 DOCUMENTATION

10.1 Log Books

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

10.2 Administrative documents

Operators will maintain a log of any event or occurrence including:

a) The operator on duty at that workstation and showing that:
   - the correct time was being displayed
   - 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.

The following shall be maintained:

- video/digital tracking register
- occurrence/incident register
- visitors register
- maintenance of equipment, whether routine or breakdown
- staff signing on and off duty
- video print log
- list of installed equipment

Appendix 'A'

Subject Data Access Form

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

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

Your Rights

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of the information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or data does not fall within the Data Protection Act 2018 or if you agree otherwise. whg will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, whg is not obliged to comply with an access request unless:

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

whg CCTV System Rights

Walsall Housing Group may deny access to information where the Act allows or does not apply. The main exemptions in relation to information held on the CCTV System are where the information may be held for:

- Prevention and detection of crime
- Apprehension and prosecution of offenders
- Where the Data Protection Act 2018 does not apply (where not used to capture identifiable individuals or information relating to individuals)

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

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

Section 1 Asks you to give information about yourself that will help us confirm your identity. We have a duty to ensure that information it holds is ensure and it must be satisfied that you are who you say you are.

Section 2 Asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, date of birth and current address) together with a recent photograph of you, unless one of the documents includes a photograph.

Section 3 The declaration must be signed by you.

When you have completed and checked this form, take or send it together with the required TWO identification documents and photograph to: The Data Protection Officer, whg, 100 Hatherton Street, Walsall, WS1 1AB

SECTION 1 About Yourself

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

PLEASE USE BLOCK CAPITAL LETTERS

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

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

SECTION 2 Proof of Identity

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

For example: a birth/adoption certificate, driving license, medical card, passport or other official document that shows your name and address. Also, a recent, full face photograph of yourself.

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

SECTION 3 *Supply of Information*

You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to:		
(a) View the information and receive a permanent copy	YES / NO	
(b) Only view the information	YES / NO	

SECTION 4 *Declaration*

DECLARATION (to be signed by the applicant)

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

Signed by _____ Date _____

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

NOW – please complete Section 4 and then check the 'CHECK' box before returning the form.

SECTION 5 *To Help us Find the Information*

If the information you have requested refers to a specific offence or incident, please complete this Section. Please complete a separate box in respect of different categories/incidents/involvement. Continue on a separate sheet, in the same way, if necessary.

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

Were you: **(tick box below):**

A person reporting an offence or incident ☐

A witness to an offence or incident ☐

A victim of an offence ☐

A person accused or convicted of an offence ☐

Other – please explain	

Date(s) and time(s) of incident	

Place incident happened	
Brief details of incident	

Before returning this form please check:
1) Have you completed ALL Sections in this form?
2) Have you enclosed TWO identification documents?
3) Have you signed and dated the form?

Further Information:

These notes are only a guide. The law is set out in the Data Protection Act 2018, obtainable from The Stationery Office. Further information and advice may be obtained from:

The Office of the Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel. (01625) 545745

Please note that this application for access to information must be made direct to whg (address on Page 1) and **NOT** to the Information Commissioner.

OFFICIAL USE ONLY

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

Application checked and legible? ☐ Application Received ☐

Identification documents checked? ☐

☐ Documents Returned? ☐

Member of Staff completing this Section:

Name ☐ Position ☐

Signature ☐ Date ☐

Appendix 'B'

CCTV SCHEME DESCRIPTION

The Data Protection Act 2018

CCTV IN OPERATION

This section contains advice and information regarding data recorded by the CCTV system and gaining access to that data.

whg
100 Hatherton Street
Walsall
WS1 1AB

THE PURPOSES FOR WHICH IMAGES ARE RECORDED

Full details of the principles and criteria under which this system operates may be found in the CCTV Code of Practice. The aims and key objectives of the system are:

The following purposes have been established for the whg CCTV and associated systems:

a) reducing the fear of crime

b) deterring and preventing crime

c) assisting in the maintenance of public order and reducing offences involving vandalism and nuisance

d) encouraging the use of the facilities offered by whg

e) providing evidence which may assist in the detection of crime and the apprehension and prosecution of offenders

f) protecting property

g) providing assistance with civil claims

h) providing assistance with issues relating to public safety and health

i) providing assistance and reassurance to the public in emergency situations

CCTV SCHEME

CODE OF PRACTICE

Copies of the Code of Practice are available free of charge on application to the CCTV System Manager.

RECORDED IMAGES

The CCTV system operates 24 hours per day, every day of the year. All cameras are continuously recorded. Images are retained for 30 days.

All recordings are retained for a minimum of period. If no legitimate requests for retention of the recording has been made it is then erased. All requests for retention of recordings are considered against the provisions of the Data Protection Act, Human Rights Act and the Code of Practice.

The storage, processing and use of the recorded data obtained by the CCTV system is guided by the following general principles.

Recorded data will only be used for the purposes defined in the Code of Practice and in accordance with the provisions of the Data Protection Act and Human Rights Act.

Access to recorded data shall only take place in the circumstances defined in the Code of Practice and the provisions of the relevant legislation.

Recorded data will not be sold or used for commercial purposes or the provision of entertainment.

The showing of recorded data to the public will only be permitted in accordance with the law in relation to the investigation, prosecution or prevention of crime.

Data released shall remain the property of whg.

DISCLOSURE POLICY

Disclosure of data obtained by the CCTV System will only be committed in accordance with the relevant legislation and the criteria contained within the Code of Practice.

In every case a written application in an approved format, clearly showing the reasons for the request is required.

The code lists third parties from who requests to view data will be regarded as ‘primary requests’ and sets out circumstances in which such applications may be made.

Third parties include:

The Police; Fire Service; H.M. Customs & Excise; whg (Specific Officers); Other statutory prosecuting bodies (e.g. Trading Standards, Ministry of Defence Police; British Transport Police; etc); solicitors; plaintiffs/defendants and persons exercising their rights of subject access under the Data Protection Act 2018 and GDPR.

SUBJECT ACCESS

If you wish to exercise your rights of subject access as provided for in the Data Protection Act 2018 you will be required to make the request in writing on a standard subject access request form.

All requests for subject access will be dealt with by the CCTV Manager or a nominated deputy. A written response to the request will be provided within 30 days of receipt, either setting out the steps intended to take to comply with the request or setting out the reason for refusing the request.

The Data Protection Commissioner has published a Code of Practice for Users of public area CCTV Systems. A copy of this code may be obtained on application to the Data Protection Commissioner.