

## Module 2: Working as a CCTV operator

### Chapter 1: The roles and responsibilities of CCTV operatives

#### Role and responsibility of CCTV staff

CCTV control rooms will vary considerably from a small shopping centre with one or two operators to larger environments, for example airports or universities with many operators and a team of other staff. Each member has a role to play and it is important we understand what each has to do. In many cases, the role will fall upon more than one member of the team, according to local practice. For example, the reviewing of CCTV images for evidence is sometimes carried out only by supervisors, but in other schemes, operators have full access to review.

#### The system owner

Every CCTV system has an owner, whether it is an individual person, a local authority or a corporate entity. Someone has to pay for the equipment to be installed and operated. The UK has over 500 town centre systems, mostly owned and operated by a local council, as well as hundreds and probably thousands of private CCTV control rooms, which may also have other functions. The owner(s) will be responsible for deciding **why and how** CCTV is to be used. They must also consider if CCTV is necessary as there are plenty of alternatives – extra staffing, better lighting, robust fencing, etc. Local authorities may also have to define a **pressing need** for CCTV under new UK legislation.

When the decision has been made to build a CCTV system the owner(s) must consider how it will be operated and managed as it is they who will have the legal responsibility for the system. Ultimately, this will depend on the budget available, but there is clear guidance now to influence the quality of images if they are to be used effectively. The system owner must also ensure that there is a suitable process of administration in place and that all the relevant documentation has been created, for example the **code of practice**, and the owner has to sign up to this along with any other partner(s) to the CCTV scheme.

#### The system manager

If the owner has invested in a CCTV system, they will want it to be effective and this is going to require careful management. In many cases, a manager will have worked

as an operator before and gained much experience in the running of a system. It is essential that they have a good working knowledge of the following topics, although this list could be extended:

- CCTV equipment and its maintenance;
- Management of recorded material;
- Staffing and human resources issues;
- Current legislation applicable to CCTV;
- Dealing with the public, especially complaints; and
- Developing the CCTV system and training staff.

#### The CCTV supervisor or team leader

In larger control rooms with numerous operators, there may be a shift supervisor or team leader. This role sits between an operator and manager and is likely to have some delegated duties from the manager included from the list above. The usual tasks will include the day-to-day running of the team of operators and dealing with minor staffing issues, for example setting shift patterns and ensuring there are sufficient staff to cover the room. They are usually more experienced operators and may have a deeper understanding of legislation to give advice to operators generally.



Each member has a role to play and it is important we understand what each has to do.



## Module 2: Working as a CCTV operator

### Chapter 1: The roles and responsibilities of CCTV operatives



#### The CCTV operator

No CCTV system can work effectively without a CCTV operator. Arguably the most important role of a system is that the operator must maintain vigilance when on duty. Although there are many technological tools available to assist, the operator can make instant decisions on what they see in front of them. CCTV operators often have to work alone which can make the role more challenging. Having good self-discipline and professional standards enables the lone worker to be efficient. Health and safety for lone workers is covered in more detail in chapter 7.

The following is a list of topics on which each operator should have at least a reasonable knowledge in order to achieve a good level of operation:

- Operation of CCTV equipment: proactive use of cameras and reactive use of cameras;
- Operation of other equipment within a control room: radios, access control, etc.;
- How to identify appropriate areas and people to monitor;
- How to carry out administrative tasks, multitasking;
- Communication with others: colleagues, other agencies, the public, etc.;
- How to conduct oneself in a professional manner in keeping with SIA standards;
- Observing health and safety rules, 'lone worker' policy;
- Attending court to deliver evidence; and
- Understanding and using legislation effectively.

#### Technical support staff

CCTV systems can be small or large. In either case, there will be a need to maintain their working effectiveness. Technical support staff will normally have some formal training in the technical characteristics of a CCTV system and there are now qualifications in the design and building of CCTV systems, given the complexity of such equipment. Often an area that is overlooked or underfunded, maintaining a fully working scheme, may be considered a requirement under The Data Protection Act 2018 which says

collecting data (images) must be processed lawfully, transparently and for a specific purpose. (Principle 3, Data Protection Act 2018). If a camera is not adequately giving clear images or is facing the wrong direction, it may not comply with this principle.



#### The data controller

Although this is discussed later in the legal section (chapter 4) the role of the data controller is important. Having an understanding of it will help the CCTV staff to carry out their role effectively. The data controller has a legal responsibility for data processed by the CCTV system.

#### CCTV and confidentiality



Confidentiality is defined as *a set of rules or a promise that limits access or places restrictions on certain types of information.*

For CCTV operators it will relate to **any information** that comes into their possession. This will include CCTV images, still images, personal information and anything that relates to operational CCTV.

Information cannot be disclosed to **unauthorised persons**, and the responsibility to disclose is on the person being asked for information to check the clearance status of the requesting person. Where a request is received from a person not known to be an authorised person, advice should be sought from a supervisor to establish the validity of the request.



## Module 2: Working as a CCTV operator

### Chapter 1: The roles and responsibilities of CCTV operatives

Where information has been unlawfully disclosed, for example CCTV images being posted on social media, the person responsible may be in breach of the law and the following penalties might apply:

- Prosecution under the Data Protection Act 2018 or other legislation by the Data Protection Authority;
- Fines or in extreme cases imprisonment;
- Loss of SIA licence; and
- Dismissal from employment.

#### Privacy

There are different levels of privacy, according to the circumstances at the time. People may be happy to have their photograph taken in a group, for example a wedding or sports picture, whereas a close-up of the family with children might not be appropriate. Home Office guidance is set out in a code of practice issued by the Surveillance Camera Commissioner which is explored further in chapter 3.

Each of us has what is known as an **expectation of privacy** which establishes what we can expect depending on where we are. In a **public place** our expectation of privacy will be low, as we can be seen by others and we are unlikely to be doing anything of a private nature. However, if we are in a **private place**, for example our rear garden, we would not want anyone to view our activity; our expectation of privacy is higher.

This is a fundamental principle of CCTV operation and all operators should be aware of it.

With the high-quality lenses and zoom capabilities of many CCTV systems it is possible to view private areas during routine operations. Some systems may be able to 'blank out' such areas as a bathroom window or bedroom and this should be used where possible. If a system does not have this capability it is essential the operator has been given some training in privacy matters.

The system should be used at all times in accordance with the proper aims of CCTV, and viewing into private areas can only be permitted for a lawful purpose. For example, if the operator receives a call from the police suggesting a criminal offence is taking place in a private area, the operator may be justified in pointing the camera into that area.

Later we will look at the offence of voyeurism, where cameras are directed at persons for sexual gratification.

Operators must be aware of this restriction to prevent possible criminal action being taken against them.

Many occurrences will not require action to be taken.

CCTV operators are made aware of incidents via a number of methods:

- Reported to CCTV operators by police or other agency;
- Reported to CCTV operators by the public;
- Pre-planned viewing – parades, carnivals, etc.; and
- Found by camera – the operator has seen something significant on the monitor(s).



We can place incidents generally into three camps:

**EMERGENCIES**

**URGENT**

and

**NON-URGENT**

Emergencies are life-threatening incidents requiring immediate attention and probable deployment of emergency services.



#### Incidents

In CCTV terms – an incident can be defined as:

**'Any occurrence that requires some action to be taken by the operator.'**

## Module 2: Working as a CCTV operator

### Chapter 1: The roles and responsibilities of CCTV operatives



The level of response for each one will be decided initially by the operator and they will have to use their judgement in keeping with any local instructions. More serious incidents and crimes should be reported with urgency, whereas minor incidents might be passed to another agency where appropriate.

For example, old damage to a town centre waste bin might be reported to the local authority in slow time, whereas, if someone was present damaging the bin at that time it is more likely to require immediate deployment.

CCTV systems can see all sorts of incidents and the operator should develop their skill in being proactive in using cameras to identify possible incidents. Suspicious behaviour is usually accompanied by someone displaying unusual body language traits. An effective CCTV operator is one who has learned these traits and can use them to identify persons who might be engaged in criminal activity. Body language is dealt with more thoroughly within the practical unit.

There may still be some action required, but the operator should consider that there may be underlying issues that are not immediately obvious, but require more urgent action. Is the traffic congestion the result of a collision and are the crowds in the street watching a crime in progress?

In all cases, the job of the operator is to get the **best possible images**. Remember, an operator cannot stop what is happening from the control room, and the images collected may be crucial in a post-event investigation. In the past, operators who have zoomed into the subject and collected identification size images have provided very important evidence to the police.

We can assist the police and other agencies by ensuring that we report clearly what we see and by getting the best possible images.



Many incidents are classed as 'non-crime' and therefore do not require the same response as crimes.

The types of incident classed as non-crime may include the following:

- Missing persons;
- Traffic congestion;
- Peaceful demonstrations;
- Parades and carnivals;
- Crowds in the street;
- Accidents/fires/evacuations;
- Floods; and
- Health and safety issues.



## Module 2: Working as a CCTV operator

### Chapter 1: The roles and responsibilities of CCTV operatives

#### Crime and disorder

CCTV operators should develop a good knowledge of the area covered by their CCTV and by doing so they can be more effective. An effective operator will try and identify areas which become active for local crime and disorder incidents. This may require close liaison with the police or other agencies (local authorities, housing associations, etc.) and also CCTV colleagues.

Areas which attract the attention of criminals include the following:



- Crowded areas – distraction thefts, pickpockets, etc.;
- ATMs – confidence tricks and tampering of ATMs;
- Sports events – pickpockets, etc.;
- Open restaurant tables – distraction thefts, bag thefts, etc.;
- Banks – confidence tricksters, distraction thefts and ATM crime;
- Car parks – distraction thefts, car crime;
- Bus/train stations – pickpockets, distraction thefts;
- Retail/business areas – office thefts, shoplifting, distraction thefts;
- High profile/local authority buildings – distraction thefts, office crime; and
- Leisure and entertainment areas, etc. – locker thefts, vehicle crime, anti-social behaviour, child protection issues.



A **hot spot** could generally be any area where the risk of crime is high. All of the listed hot spots could be considered as crime hot spots, but the effective CCTV operator will be able to identify anywhere **the risk of crime** is heightened. For example, an elderly lady at an ATM in company with a man dressed in a workman's high-visibility jacket might suggest a confidence trick in progress. A common crime involves workmen getting elderly residents to pay large amounts of cash for work never undertaken. An operator identifying this type of activity may well feel it is appropriate to contact the police.

In trying to identify the risk of a crime hot spot, some of the following factors (and others) may contribute to that decision:

- Time of day – rush hour versus quiet periods;
- Dark areas versus well-lit areas; and
- Remote areas versus well-populated areas.



## Key Task 1

- 1 David is a CCTV operator who has just started working for a security firm in a busy CCTV control room at a shopping centre, where they have the contract to provide security. He has never used CCTV before and is given instruction on the equipment by his supervisor. Write down 3 things that you think David's role will involve:

1

2

3

- 2 Record 3 examples of Non-Crime Incidents and 3 examples of Crime Incidents:

1

2

3

1

2

3

- 3 State 3 different factors that might influence an area becoming a crime 'hot spot':

1

2

3

## Module 2: Working as a CCTV operator

### Chapter 2: Characteristics and equipment of a CCTV system

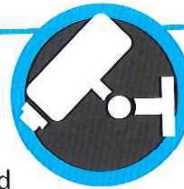
#### CCTV equipment

CCTV has continued to develop over the last decade and some systems contain complicated electronic equipment, but the basic CCTV system could consist merely of a few components.

Modern systems tend to be digital in their make-up compared with the older and less used analogue systems. Digital systems use computer-based technology whereas analogue makes use of the video tape recording equipment which still exists, but is slowly being replaced.



A basic system will comprise the following:



Camera(s) connected by some method of transmission to some type of monitor and possibly a recording method.

A CCTV system includes all or some of the following pieces of equipment:

- **Camera(s)** – fixed, pan, tilt and zoom (PTZ), dome, box;
- **Lens** – manual, auto iris, zoom, fixed;
- **Control systems** – joystick, keyboard, touch screen;
- **Transmission methods** – copper wire cable (twisted pair), fibre optic, coaxial cable, infrared, microwave and radio, Internet protocol (IP) transmission;
- **Monitors** – older cathode ray tube (CRT) screens, flat screens – light emitting diode (LED), thin film transfer (TFT), liquid crystal display (LCD and plasma), projectors;
- **Recording systems** – video cassette players (old technology) digital video recorders (DVR) and network video recorders (NVR), flash drives, memory sticks, secure digital (SD) cards, compact discs (CD) and digital video discs (DVD), mobile phones, etc.;
- **Matrix and multiplexer systems** – allow numerous or single camera signals to be routed into different recording or monitoring areas and they can change the format of video signals in some cases; and
- **Printers** – digital laser, inkjet, photographic.



#### Cameras

CCTV cameras first started being used in 1942 by the Germans to observe rockets being launched towards the UK. In the 1950s they were developed in America for medical use. Since that time, CCTV cameras have developed to a very high standard, with ultra-high-definition cameras being used on spacecraft and satellites as well as now being used in CCTV systems around the world.



## Module 2: Working as a CCTV operator

### Chapter 2: Characteristics and equipment of a CCTV system

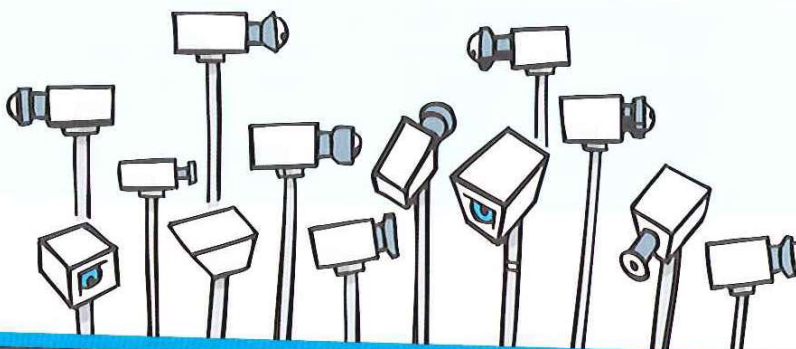
#### Types of camera and their likely employment

(Figure 1)

The following chart shows the different types of camera and likely employment of those cameras:

Type of camera or housing	Details and use
<b>Black and white</b>	Generally older cameras but some modern cameras go to black and white (see day/night cameras). Used in all areas.
<b>Colour</b>	Cameras processing colour images. They require sufficient light to process colour. Used in all areas.
<b>Day/night</b>	Cameras that produce colour in daylight but when light levels drop below a certain level change to black and white images. Used in all areas.
<b>Fixed</b>	Cameras fixed to view one point only, usually doors, corridors, alleyways, etc.
<b>Pan, tilt and zoom (PTZ)</b>	Cameras that can be moved by the operator – left and right (pan), up and down (tilt) and moved to give close-up views (zoom). Used in all areas but especially where zooming in and following moving persons/ vehicles is required.
<b>Analogue</b>	Older camera technology but images can be sent to digital recording systems. Limited quality as images are made up of television lines (TVL). Used in all areas.
<b>Digital</b>	Cameras that produce images that use computer technology and compiled using pixels. High quality possible. Used in all areas.
<b>High definition</b>	Digital cameras capable of producing high definition images made up of large amounts of pixels.
<b>Ultra high definition</b>	Digital cameras now capable of very high definition images. Used in all areas.
<b>Infrared</b>	Cameras using infrared light technology. Infrared light is very high frequency light that the eye cannot see but cameras can. Used where night-time views are required with zero lighting available.

The principle of how a CCTV camera works is similar to the different technologies giving different standards of image.





## Module 2: Working as a CCTV operator

### Chapter 2: Characteristics and equipment of a CCTV system

#### Lens

At the front of any CCTV camera is a lens. This is an optical method of allowing light to transfer through it on to the camera processing system inside. A lens is used to ensure the image is in focus and a more complex lens allows for a camera to be zoomed into a close-up view. Inside many CCTV lens units is a mechanism that increases or reduces the amount of light that enters the lens. This is called the iris and in most modern lens units, it will operate automatically, so that when the light level increases the iris closes up, reducing the amount of light entering and vice versa.

The type of lens also gives us the various zoom capabilities and these allow images to be brought into close-up view. Generally the higher the number of ratio, the closer the image can be obtained.

Digital imaging also allows for a zoom capability, but does not involve varying the lens, but takes place electronically by zooming into the image which has been recorded.

#### Image sensor

Modern cameras have some form of imaging sensor inside. This is a small panel that the lens directs its image on to and modern cameras tend to use two types of chip – a charged coupled device (CCD) and a complementary metal oxide semiconductor (CMOS).

#### Transmission

The images a camera produces need to be sent to a monitor somehow. This is usually transmitted by way of a cable and each camera will have some form of transmission output at the back. Many systems also have wireless transmission systems including satellite connection.

#### Emerging CCTV technologies

There are a number of new and emerging technologies which can assist how CCTV operates. They are continually developing and improving and many are already used in public space surveillance.

Digital recording is widely used and is fast replacing the older analogue technology which made use of videotapes. Digital Video Recorders (DVR) and Network Video Recorders (NVR) save the image data in the form of a computer data file which can then be processed by software on the computer. It has many advantages over analogue, and is much quicker to search when looking for specific events.

Large amounts of recorded material can be stored using digital technology whereas videotapes can take up huge amounts of storage space and their storage conditions must be observed to maintain their quality.

There are many different types of DVR and NVR and standards of quality will vary. They can be technically complicated to operate, and using digital recording equipment will require the CCTV operator to undergo training, normally part of their induction process.

European standards do exist for the control of image quality and there are Home Office guidelines which set out the expected quality of images produced for evidence. These are technically complex and students may wish to undertake further reading to study them although they are not tested for SIA licence purposes.



#### Power

All cameras will need some form of power (electrical) to work. Modern cameras tend to be low voltage, generally 12 or 24 volts DC current.



## Module 2: Working as a CCTV operator

### Chapter 2: Characteristics and equipment of a CCTV system

**Algorithms** are computer processes that may be able to identify irregular activity on the screen. For example, when a person loiters near to parked cars or leaves a bag

unattended at a bus stop, the computer identifies that this is unusual activity and alerts the CCTV operator, see behaviour recognition.

**ANPR (automatic number plate recognition)** is the use of a computer to automatically screen vehicle registrations using the CCTV camera. This compares the vehicle number with a database and indicates to the operator what the interest is in the vehicle. Cameras have to be set up specifically to read number plates. The police make great use of ANPR and when vehicles pass through a camera which identifies an issue, they deploy officers to stop the vehicle.

Other ANPR uses include car park management, access control and petrol station forecourt management. Details of vehicles that have stolen fuel may be in the petrol station's database which will indicate this to the cashier when the vehicle pulls on to the forecourt.



**Facial recognition** (biometric) is now being used by advanced CCTV systems to identify individuals from their facial features. The face is encoded by the computer to give a specific number, which is compared on a database. Border control staff make great use of facial recognition on passport controls at UK airports.

**Biometric recognition** includes other methods of identifying persons from some personal details, for example by using their iris pattern, fingerprint details, palm print and even by way of voice recognition. Recognising clothing is also now possible by CCTV with the logos, colour and types of clothing being held on databases in police records.

**Motion detection** is the method by which a CCTV system recognises when there is some change in the image. In a digital system, pixels will change as something or someone moves across the screen. This is mostly used to reduce the amount of space required to store data and the system will not record unless there is movement. An automatic process, it can be set up to warn the operator of a screen change from cameras that might not be monitored at that particular time. For example, a doorway (or many) at night might be

monitored by a camera with motion detection, and automatically record and bleep at the operator to show activity. It is unlikely that an operator might be required to sit watching many doorways at night, particularly if there are a large number being monitored by cameras.

## Module 2: Working as a CCTV operator

### Chapter 2: Characteristics and equipment of a CCTV system

**Behavioural recognition** patterns are being developed on some systems. The computer monitors a person's behaviour and movements and alerts the operator when something different is carried out by the subject of the image. This is carried out by a complex computer algorithm programme and is usually set up to cover specific areas, for example high-value locations or areas with a high security risk. The system works by recognising actions rather than individuals. Some behaviour patterns, for example crowds running or converging in certain places, are known as 'trigger events' and they set off a chain of events within the system. If someone pulls out a gun, people are likely to scatter haphazardly and the system can recognise the crowd scattering as a trigger event indicative of some kind of problem.

#### Public address systems (PA)

Some public space CCTV is now making use of public address systems in conjunction with cameras. The operator identifies someone acting suspiciously and can speak directly with them using the PA. Often used by town centre systems to deal with rowdy behaviour, the CCTV operator gives a voice warning to the persons concerned.

In many control rooms all voice traffic (radio, telephone, PA, etc.) is recorded using digital technology, often to assist in post-event incident investigations.

**Thermal scanning cameras** are used in high-risk areas and to identify a change in temperature. Widely used on police helicopters and by the military they show an object temperature in relation to the surrounding area. This makes them ideal to identify a person hiding from police for example. The warm body temperature will show up as a different colour to a colder surrounding area.

#### CCTV systems failure

Given the large amount of technology used in a CCTV control room, it is highly possible that there will be a systems failure (full or part) at some time. In the event of any systems failure then the local procedures should be followed, but an operator should remember that maintaining safety and security of the control room is essential.

If access control fails, operators will have to manage any entry to the room manually.

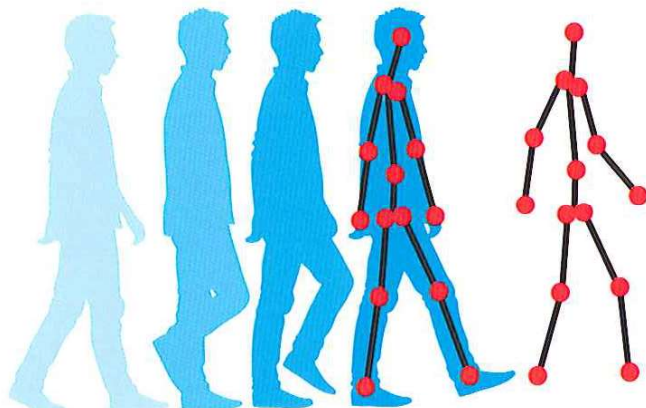
CCTV systems may or may not have a back-up power facility process but in most cases the appropriate action might include contacting engineers and making a fault report. An entry should always be made in the operator log for such failures. Fault reporting is covered fully in chapter 8.



#### Mobile CCTV solutions

Many town centre organisations and police forces make use of mobile CCTV units whereby vehicles are fitted with CCTV cameras and used to patrol areas. Vehicles can vary from a small saloon car with a single camera to a larger van with on-board control room facilities. These are flexible and can be deployed at short notice to manage areas not fitted with pole cameras or wired systems.

**Gait recognition** is the identification of a person from the way they walk. Research into gait recognition is continuing and researchers believe it has tremendous value to offer CCTV systems.



## Key Task 2

- 1 Give 3 examples of the different ways in which images can be transmitted for CCTV systems:

1

2

3

- 2 Give 3 examples of the different types of CCTV camera a system may use:

1

2

3

- 3 Give 3 examples of new technology being used in CCTV systems today:

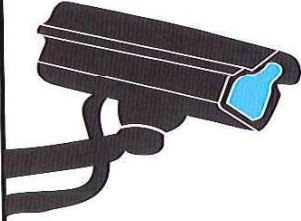
1

2

3

## Module 2: Working as a CCTV operator

### Chapter 3: CCTV codes of practice and operational guidelines



**CCTV codes of practice, operational procedures and guidelines**

A code of practice can be defined as:

*'a set of written rules which explains how people working in a particular profession should behave.'*

In addition, a code of practice sets out the valid reasons that CCTV may be used.

(Figure 2)

## The reasons that CCTV may be used

The following chart sets out clearly the reasons for CCTV being deployed in accordance with the codes of practice and how that specific use can be instigated by the operator. It is essential that CCTV operators know the reasons for their particular system as it may vary and have other purposes included in the code of practice.

Key purpose	How it is achieved
<b>Prevent crime</b>	By being a clear and visible deterrent to would-be offenders (camera signs and visible cameras, etc.).
<b>Detect crime</b>	By providing clear and accurate images of offenders, suspects and witnesses and showing a visual account of the incident or event. Providing quality evidence to investigators in the form of recorded images with sufficient detail and image sizes to identify offenders, suspects, etc.
<b>Provide and enhance safety and security in the environment</b>	By having a manned system of cameras watching for risks to people and property. CCTV allows the public to feel that they are in a safe and secure environment.
<b>Assist in managing an area</b>	Providing real-time information about the area being monitored thus allowing quick decisions to be made. For example – health and safety risks requiring urgent attention.
<b>Traffic management</b>	Assisting in the managing of vehicles for an area being monitored. For example – a university campus where there are many vehicles moving around.
<b>Access control</b>	Part of the overall security purpose, but widely used to identify visitors to premises and confirm identity before access is granted.
<b>Any other purposes</b>	CCTV <b>may</b> be used for other reasons that are not included in the above, provided they are <b>LAWFUL</b> and <b>REASONABLE</b> . Monitoring the public in public places will be slightly different to using cameras in a private workplace, for example measuring the output from a workforce. This type of use has other considerations before it should be undertaken.

## Module 2: Working as a CCTV operator

### Chapter 3: CCTV codes of practice and operational guidelines

CCTV systems have to operate according to a number of different documents and guidance papers. These guidance papers may be advisory, but legislation introduced in 2012 has made it a requirement for some CCTV systems to adhere to legal procedures. There are different codes of practice available for CCTV systems, but the two main codes that operators need to adhere to are:

- The Information Commissioner's CCTV Code of Practice; and
- The Surveillance Camera Commissioner CCTV Code of Practice.

Most CCTV systems will use the above codes to develop their own code, which will be specific to their own particular scheme. All are considered public documents and should be made available for the public to view upon request and to be informed about CCTV.

The purpose of the Information Commissioner's CCTV Code of Practice, issued under the Data Protection Act is to give members of the public reassurance that the system is being used fairly and lawfully and that it is run with integrity. It sets out advice on how the system should be operated and what happens to recorded material and allows for the public to request access to their personal data (images) using the proper process.

This code specifically covers the use of camera-related surveillance equipment including:

- Automatic Number Plate Recognition (ANPR);
- Body-worn video (BWV);
- Unmanned aerial systems (UAS); and
- Other systems that capture information of identifiable individuals or information relating to individuals.

The Data Protection Act 2018 requires the CCTV owner to notify the Data Protection Authority (ICO) that they are processing data and a sliding scale of fees will apply. This now includes home domestic CCTV systems where they can view **outside** of the household boundary into other areas, for example the road or a neighbour's garden or doorway.

This code provides guidance on information governance requirements, such as data retention and disposal (including using the cloud to retain data) which is important to follow in order to comply with the 6 data protection principles (see chapter 4).

This code also provides good practice advice for those involved in operating CCTV and other devices which view or record images of individuals. Following this code will ensure that the operators and system owners comply with the legislation and help to prevent accusations of malpractice.

The Surveillance Camera Commissioner Code was established under the Protection of Freedoms Act 2012 and applies currently to **relevant authorities**. It has the same broad aims as the Data Protection Code, to ensure integrity and reassure the public. This code only applies to relevant authorities, currently local authorities and police forces and does not apply to private CCTV systems, although the Commissioner recommends the code is adopted by them. This code sets out to engage local communities and to give them confidence that cameras are being deployed to protect them, not to spy on them. There are 12 guiding principles in the code.



## CCTV Codes of Practice

These 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 on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
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 effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be 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.

Operational procedures and guidelines are established or prescribed methods to be followed routinely when using CCTV is required. Often referred to as **assignment instructions** they set out the day-to-day running instructions for a CCTV system. These procedures will be considered private documents and are not made available to the general public.

Each CCTV scheme will have its own set of operational procedures that will be specific to local procedures and processes.

When operators comply with the code of practice and operational procedures, the impact of doing so will include the following:



- Evidence gathered is more likely to be admissible in a court;
- The public will be reassured and confidence in CCTV will be raised;
- Help ensure that those capturing individuals' information comply with the DPA and other relevant statutory obligations;
- Help inspire wider public trust and confidence in the use of CCTV;
- Standards will be maintained or raised;
- Contribute to the efficient deployment and operation of a camera system;
- Help organisations in England and Wales to follow guidance in the Protection of Freedoms Act code;
- Partners and other agencies will have a clear understanding of working relationships; and
- Operators will be protected from allegations of CCTV misuse.

## Module 2: Working as a CCTV operator

### Chapter 3: CCTV codes of practice and operational guidelines

CCTV operators should be aware that non-compliance with these codes and procedures may have consequences for themselves and the organisation. When CCTV is misused it may be a breach of the law, resulting in prosecution. Operators should therefore ensure they are familiar with the contents of their code of practice to avoid placing themselves in such a position. Operators must adhere to the SIA standards of behaviour discussed in Module 1 at all times and provide a professional and effective service.

#### Selecting subjects to view with CCTV

During routine CCTV use, the public are viewed in general terms and operators then identify activity which requires a closer look. Operators may know the person in view and have previous experience of their criminal activity or there may be intelligence suggesting illegal activity. In most cases, the person is seen doing something suspicious or illegal or their body language suggests that closer surveillance is required. In some cases, it may be necessary to pre-plan surveillance and target someone. This is usually carried out at the request of the police or other agency, for example Revenue and Customs.

In some cases surveillance will require specific permission before it can be carried out and UK legislation places a requirement upon CCTV operators to obtain authority under the Regulation of Investigatory Powers Act. RIPA in Scotland (see chapter 4).

The code of practice sets out the proper reasons why we make use of CCTV and the operator should always use cameras in accordance with the code of practice. Targeting of people and vehicles should be justified and surveillance should be fair and lawful in keeping with the chart in figure 2.

**Targeting and tracking** is much more than merely viewing a subject. Targeting and tracking is when you use cameras to follow a person or vehicle more closely. This might include watching someone loading up their car, vehicles being driven in circumstances that suggest criminal activity or following the activities closely of persons and obtaining close-up images.

Operators should consider the rights of the public when viewing and the Human Rights Act and Data Protection Act should be borne in mind at all times when carrying out surveillance. These set out what rights a person has in respect of their privacy and information.

If an operator is targeting a person because of something seen that could be suspicious, then if no criminal activity or other valid reason to continue monitoring is present, the operator should resume normal activity. Operators should always be aware of the rights of people to carry on their daily life without unnecessary surveillance into their activities.

From time to time covert surveillance may be required. The Regulation of Investigatory Powers Act (RIPA) provides a legal authority for this to be carried out when correctly authorised. If surveillance is being carried out under an authorisation from RIPA then images will be required in accordance with that authorisation, and may include general non-criminal activity. More information on RIPA is contained in chapter 4.

In addition to the effective use of cameras by an operator, technology has produced a number of additional tools to assist.

#### Automatic Number Plate Recognition

(ANPR) is a method by which cameras automatically scan a vehicle registration number and compare it to a database. Where the vehicle number has been flagged for some reason, the operator will be alerted to then initiate further action. This is most commonly used by the police when looking for stolen vehicles or vehicles without insurance, for example.

When a car number plate has been flagged by the system, it is essential that a human comparison is also made between the image and the database to avoid deploying police or security when a misread has occurred (perhaps due to a dirty number plate for example).

**Facial recognition** is a method whereby the camera obtains a close-up view of someone's face and the system converts the image to a digital reference, which is again compared to a database. The database will have details of persons who are wanted contained within it, or it may just be used for access control. Revenue and Customs uses this system at some airports now to confirm arriving passengers are bona fide residents.

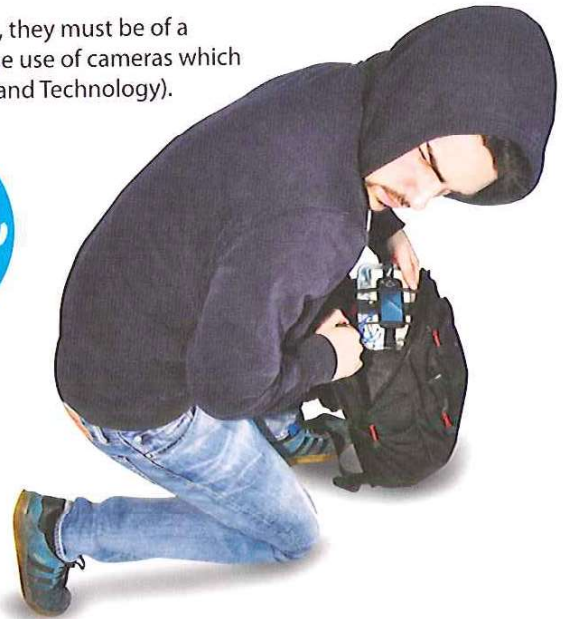
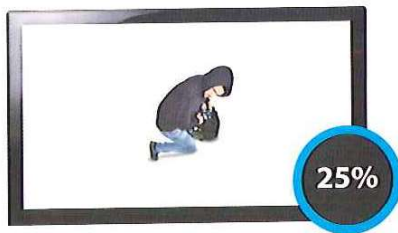
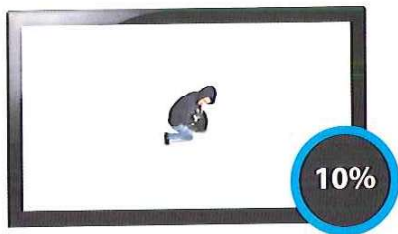
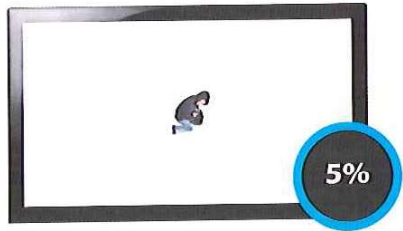




## Module 2: Working as a CCTV operator

### Chapter 3: CCTV codes of practice and operational guidelines

In all cases, if the images are to be used for investigation purposes, they must be of a suitable size to do so. There are some guidelines appropriate to the use of cameras which have been issued by the Home Office (Centre for Applied Science and Technology).



A practical application for operators to assist the investigator is to obtain a close-up image of persons or vehicles even if, at that time, there is no reason to suspect criminal activity. For example, obtaining close-ups of the people queuing to go into a nightclub will place the detail into the recording system. If, later in the night, an assault takes place in that area, the investigator now has images of persons who may or may not be involved.

In large-scale incidents, for example riots, the investigator will want close-up views (100%+) to identify the offenders but a police commander might want a wide angle view to get a better view of what the crowd might be doing. Each situation will depend on a number of circumstances and the skill of the operator.

**Anomaly detection software** allows CCTV to automatically detect when suspicious activity is taking place and then warns the operator, who can look more closely for criminal activity.

**Gait recognition software** again uses a computer programme to identify the way in which a person walks. This process is quite new and still being developed, but has potential to identify a person who merely walks past a camera.

**Motion detection** is commonly used to reduce the amount of data recorded, but is also a useful tool to indicate to an operator when someone is moving in a specific area. Systems can be set up to change to the camera where the activation has occurred, thus alerting the operator to activity.

Another technique, which operators can use, is to set up cameras to cover a wide area and to try to get an overlap between adjacent cameras. This will help to keep a subject in view as they leave the view of one camera and move into another and so assist in proving the actions of the subject.

## Module 2: Working as a CCTV operator

### Chapter 3: CCTV codes of practice and operational guidelines

#### Control room security

There are a number of reasons why security of the CCTV control room is essential:

- Confidential information may be displayed on screens or discussed on radios or telephones;
- The provisions of the Data Protection Act 2018 require data to be kept securely;
- Traumatic images could be displayed on monitors;
- Incidents may be taking place requiring security or police involvement;
- To prevent access by unauthorised persons/criminals; and
- To safeguard CCTV staff and associated equipment from attack.

There are occasions when visitors may be allowed into the control room, but they must have a valid reason to enter, for example a police officer or other agency staff, solicitors to view images (which should be done in a separate viewing area) or CCTV engineers.

#### Access control systems

Control room security needs access control, which can take various forms.

Manual systems include:

- Doors opened from the inside by staff;
- Airlock systems – checking ID before access is allowed;
- Push button locks; and
- Slide bolts.

Electronic systems generally record details of who has entered or exited and include:

- CCTV – audio visual links;
- Electronic keypads;
- Card swipe systems;
- Proximity cards; and
- Facial recognition or other biometric systems.

Some control rooms may have a combination of more than one method.



#### Visitors to the control room

Any visitor to the control room should have a valid and lawful reason and have their identity confirmed by control room staff. Visitors must sign in and out for security and health and safety reasons, and appropriate documentation should be in place. It is good practice to have a confidentiality agreement signed by the visitor before access is granted.

In the case of persons who may not be authorised to enter, the reasons should be notified to the person and, in cases of criminal activity, the police may need to be informed and other immediate action may be required. This will be necessary if persons are trying to force their way into the control room to try and take over the cameras. In all cases, a supervisor should be informed and an incident report (if required) should be made.

#### Record keeping

Whilst a CCTV system is capable of recording images and storing them for later use, the operator has to be conscientious in the keeping of written records. Whilst the most important role of an operator is to get the best possible images, there is a need to maintain accurate and detailed notes and records about an incident and the day-to-day running of a system. This will include any rough notes which may be required by an investigator afterwards.

The chart on the next page shows a selection of records which should be kept and the reasons for doing so.

There may be other records to complete and this will depend on the local procedures and guidelines.

All notes and records should be taken accurately. If a mistake is made, the error should be crossed out with a single line and initialled. This helps to show that the error has been corrected only by the writer.

Notes should, if possible, be made at the time or as soon afterwards as practicable. It is not always possible to make notes when the operator is busy working with cameras, but the principle is that notes made at the time will be more accurate than trying to remember facts sometime later. Where colleagues are available, it is good practice to get their assistance.

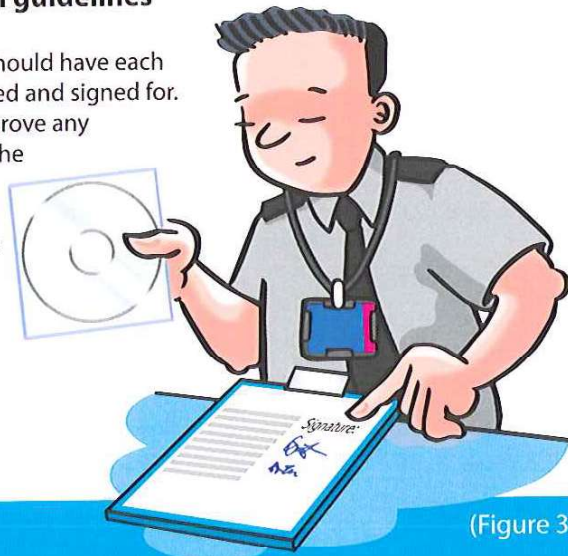
## Module 2: Working as a CCTV operator

### Chapter 3: CCTV codes of practice and operational guidelines

If notes and records are inaccurate or misleading, the consequences for the quality of the evidence will be apparent. A prosecution may be lost due to poor record keeping or inaccurate time details or where the records contradict what the images are showing to the court.

When CCTV evidence is used in court, there must be in place an **audit trail** which is a process that proves the integrity of the evidence being produced. For example, a DVD handed to a police officer, who then hands it to another police investigator to

use in the case, should have each handover recorded and signed for. This helps to disprove any suggestion that the DVD has been tampered with or left for anyone to view and possibly edit.



(Figure 3)

### Example records

Below is a selection of records which should be kept and the reasons for doing so:



**Visitors to the control room register**

To ensure only authorised visitors are given access and to comply with fire safety rules.



**Fault record log**

To report faults and report to the relevant department for proper maintenance of the system. A poorly maintained system will lose integrity in a court room. Records may be required by a court to prove a system status.



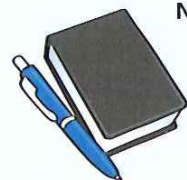
**Daily occurrence log**

This is often used to record the day-to-day (non-incident) administrative activity in a control room. Usually a chronological record of who starts a shift, when breaks are taken, visitors to the control room, etc. It does not normally contain evidential material.



**Incident log**

Details of the incident being viewed where the event is likely to require written details to compile a police statement later on. This may be required as part of the evidence for court.



**Notepads**

In most control rooms, operators keep notepads on the desk for making quick notes and scribbles about incidents and other daily information. It is possible that these could form part of the evidence chain if, for example, descriptions or car registration numbers are written down in the first instance perhaps from a radio message or telephone call. It is more likely these notes will be accurate as they have been taken at the time the information was passed.



**External viewing log**

Required to record details of who has attended *and viewed* CCTV images, for example a solicitor or police officer.



**Police statements**

A formal document required by the police when an operator produces CCTV evidence. Chapter 8 deals with the writing of statements and what should be included.

## Key Task 3

- 1 Joan, a CCTV operator for a town centre CCTV system, has been asked by her neighbour to spy on someone who has been causing her neighbour some problems. She would like Joan to follow her around the town centre and record what shops she goes into, giving her a copy of the footage afterwards. Is this allowed? If not, why not? *Record your comments below:*

- 2 The Surveillance Camera Commissioner's code of practice sets out reasons for the proper use of cameras. *Explain what each of the following words or phrases means in respect of CCTV:*

Legitimate aim =

Specified purpose =

Accountability =

Restricted access =

Transparency =

- 3 If the code of practice is followed closely, what is the impact on any CCTV evidence that is collected by an operator?

- 4 Write down 3 examples of why a CCTV operator using cameras might wish to target and follow a person:

1

2

3

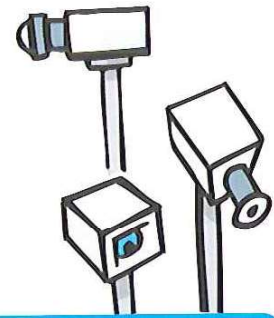
## Module 2: Working as a CCTV operator

### Chapter 4: CCTV and relevant legislation

#### CCTV and relevant legislation

There are a number of Acts of Parliament that impact upon CCTV systems. The chart below sets out the different legislation and briefly how it affects CCTV. More detail is shown at the end of the chart.

Operators should make themselves familiar with the general principles of each of these Acts of Parliament in order to be effective and remain within the law when operating CCTV.



(Figure 4)

## CCTV and relevant legislation

Act of Parliament/Legal Directive	General Topic	Brief Detail of Topics
Data Protection Act 2018	Control of data (images) Collection of images in public, Code of practice	6 Principles of the Data Protection Act 2018
Human Rights Act 1998	Privacy issues Articles 3, 5, 6, 8 and 14	Fair trial, degrading treatment, privacy at home, discrimination, etc.
Regulation of Investigatory Powers Act 2000 (RIPA), (RIPSA) 2000 in Scotland	Covert surveillance only	Directed and Intrusive Surveillance authority
Criminal Procedure and Investigations Act (CPIA) 1996	Disclosure of evidence to all involved	Audit trails, integrity of evidence, continuity of evidence
Police and Criminal Evidence Act 1984 (PACE) (Not applicable in Scotland)	Statements, collection of evidence fairly, exhibits	Documentary evidence, exhibits, identification procedures
Sexual Offences Act 2003 (Sexual Offences Scotland Act)	Voyeurism	Viewing, recording for sexual gratification
Freedom of Information (FOI) 2000 (Freedom of Information (Scotland) Act)	Statistics, general information, policy documents for CCTV	Not personal data, statistics and general information only
The Private Security Industry Act 2001	Regulation and licensing of contracted security operators	CCTV licensing, front-line licence, lasts 3 years Developing business licensing
Protection of Freedoms Act 2012	CCTV Surveillance Camera Commissioner, Code of Practice	New code of practice – statutory instrument

#### The Data Protection Act 2018

The Data Protection Act 2018 sets out how we should handle people's data (information).

In CCTV terms, this equates to many of the images recorded by CCTV systems and other personal details we might come into possession of during our work.

For an image to become **personal data** it must show sufficient details to identify the individual. A distant view showing

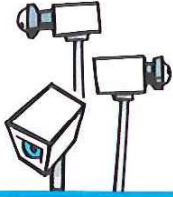
a small image of a person may not allow identification of that person and so may not be personal data. A good 100 percent image size (provided it is clear and in focus) will usually allow identification and thus become personal data.

It should be remembered though, that a small image in high-density resolution could be magnified to give a clear identifiable image, and so become personal data requiring more control and security.



## Module 2: Working as a CCTV operator

### Chapter 4: CCTV and relevant legislation



The provisions of the Data Protection Act 2018 require CCTV systems owners (who process CCTV data) to notify the data protection authority (the Information Commissioner's Office), the body responsible for overseeing data

protection legislation in the UK. This may now include domestic CCTV systems where they see into neighbours' properties. Each system should have a **data controller** who is legally responsible for the data processing.

## Data Protection Act 2018 – 6 Principles

(Figure 5)

6

Under the Data Protection Act 2018, the 6 principles set out the main responsibilities for organisations. In short, Article 5 of the regulation requires that personal data should be:

### Data must be:

- 1 Processed lawfully, fairly and in a transparent manner
- 2 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- 3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- 4 Accurate and, where necessary, kept up to date
- 5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- 6 Processed in a manner that ensures appropriate security of the personal data

### Impact on CCTV systems

There are 6 lawful basis for processing: *Consent, Contract, Legal Obligations, Vital Interests, Public Task and Legitimate Interests*. CCTV is used to protect the public, which generally falls under Vital interests and Public Task basis.

Reasons for processing will include preventing, detecting and prosecuting criminal offences, safeguarding and preventing threats to public safety.

Cameras should view relevant areas for the purpose(s) it has been placed and give clear images.

Date and time data and colour scaling should be accurate.

Data kept for no longer than is required for the purposes collected.

Data should be protected by security methods to prevent *Personal Data Breaches* either accidental or deliberate disclosure of data.

The act allows for any person to make application to the public authority for information, which can include *'any information held by the authority at the time of the request'*.

### Freedom of information legislation

The Freedom of Information Act applies only to **public authorities** and CCTV being operated by a public authority will fall under the authority of the act the definition of a public authority under this act is complex and operators might need to check with their data controller to confirm if they operate for a public authority or not.

There are some types of information which would not be released, but for CCTV operators the most important reason to restrict information under this act is that the

information requested contains personal data which, as we have already discussed, must be controlled under the Data Protection Act 2018.

Information may also not be released if it falls into one of the following categories:

- Subject of an ongoing criminal investigation;
- Interests of national security and defence;
- Information that is sub judice (information being considered by a court);
- Legal privilege; and
- Commercial interests.

## Module 2: Working as a CCTV operator

### Chapter 4: CCTV and relevant legislation

Any request for information under this act will normally be dealt with by the public authority data controller.

Requests for information can be by letter, email or other means, provided

a reply address is included by the person requesting, who may be anywhere in the world and does not have to make the request in English. Time limits are in effect to reply to the person requesting.

#### Human Rights legislation

The Human Rights Act 1998 ('the Act') applies to all public authorities (for example, central government departments, local authorities and NHS Trusts) and other bodies performing public functions (for example, private companies operating prisons). These organisations must comply with the Act – and a person's human rights – when providing a service or making decisions that have a decisive impact upon a person's rights.

Although the Act does not generally apply to private individuals or companies (except where they are performing public functions), sometimes a public authority has a duty to stop people or companies abusing a person's human rights. For example, a CCTV operator working for the local authority who witnesses a child being abused has a duty to protect the child from inhuman or degrading treatment.

The term **public authority** means more than just your local council, police or prison service. Instead, public authorities can be divided into two groups – those that provide **core (pure)** public services and

those that provide **functional (secondary)** public services:

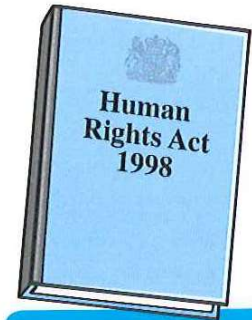
#### Core (pure) public services

Police, fire, central or local government, courts, prison service, etc.

#### Functional (secondary) public services

An individual, private business or private body that would not normally be considered as a public service, but is providing a service at the request of the state. This could apply to contractors in health care, education or the prison sector amongst others. It also includes any organisation in direct receipt of public monies.

The definition can be extensive, and is constantly growing, but may include an organisation operating a CCTV or surveillance system in a public place. It can also cover private premises (such as shopping centres, supermarkets, shops, leisure centres, pubs) operating systems that have been funded by or linked to local and national enforcement and security organisations or initiatives.



#### Examples

A police officer or magistrate in court is a **core public authority**.

A security contractor providing guarding services in UK prisons (at taxpayer's expense) **would** be considered as a public authority under this legislation.

Rolls Royce producing cars and plane engines **would not** be considered a public authority as no public service is being provided on behalf of the state.

## Rights relevant to the operation of CCTV

(Figure 6)

The following rights are relevant to the operation of CCTV for the reasons given:

Article	Title	Impact
3	Prohibition of torture (Absolute)	This is about not using CCTV in a degrading manner, for example using cameras to view female anatomy inappropriately.
5	Right to liberty (Limited)	A person's right to move around freely should not be interfered with <i>unless</i> they are arrested or sent to prison. CCTV can be instrumental in that process.
6	Right to a fair trial (Absolute)	Persons must have a fair trial within a reasonable time. Images used as evidence should be obtained within the law.
8	Right to respect private family life, home and correspondence (Qualified)	CCTV should not be used (without proper lawful authority) to intrude into a person's private family life. As a qualified article, there may be occasions when it can lawfully be used for this purpose (see RIPA page 62).
14	Prohibition of discrimination (Qualified)	In respect of the other rights in the convention, no one should be discriminated against because of their ethnic group, gender, etc.

## Module 2: Working as a CCTV operator

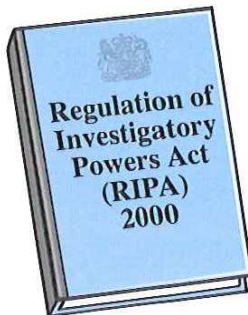
### Chapter 4: CCTV and relevant legislation

Articles are described as:

- **Absolute** means that they cannot be limited or restricted by the state under any circumstances.

- **Limited** means they may be limited under specific and finite circumstances.

- **Qualified** rights are those which require a balance between the rights of the individual and the wider community.



In respect of Article 8: *'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.'*

Surveillance which may require one or more of these Human Rights to be breached, may be authorised in very limited circumstances using the Regulation of Investigatory Powers Act (**RIPSA in Scotland**) and this is dealt with below.

#### Covert surveillance

##### The Regulation of Investigatory Powers Act, 2000 (RIPA) (RIPSA in Scotland)

amongst other things, sets out the lawful way in which surveillance may be carried out. When CCTV surveillance is requested in breach of Article 8 above, authority has to be obtained in order to do so lawfully. This legislation (RIPA) relates to the use of CCTV in two types of **covert** surveillance only. Covert CCTV is when cameras are used to view persons without their knowledge whereas **overt** CCTV (public space cameras in full view of the public) is not regulated by this act.

**Intrusive surveillance** is when viewing takes place in a residential premises or a private vehicle and the person carrying out the surveillance or the camera is present in those premises or vehicle. Public space CCTV will not be involved in this surveillance because it requires a camera to be inside a house or vehicle and not merely looking into the premises or vehicle.

**Directed surveillance** is when surveillance is carried out as part of a specific investigation or operation, and is likely to obtain private information about a person and is otherwise than by way of an immediate response to events. Directed surveillance is usually pre-planned but may, on occasions, be an urgent response to circumstances.

If the surveillance is to be carried out by a local authority (Council area in Northern Ireland), a magistrate must approve it and local authorities can only apply to use directed surveillance to prevent or detect

criminal offences that are either punishable, whether on summary conviction (magistrates' court) or indictment (Crown court) by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco.

The conditions that must be met for the police (or non-local authority) to authorise directed surveillance are set out clearly in the act and state that the surveillance must be one or more of the following:

- In the interests of national security;
- For the purpose of preventing or detecting crime or of preventing disorder;
- In the interests of the economic well-being of the United Kingdom;
- In the interests of public safety;
- For the purpose of protecting public health; and
- For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.

The following examples give two circumstances where directed surveillance is carried out:

#### Example one:

*CCTV is requested by the police to view the doorway of a house and log all persons entering or leaving without their knowledge over a period of time. This would be directed surveillance and require authorisation by a senior police officer.*

#### Example two:

*The local authority wish to obtain details of the customers (using CCTV) of a particular shop over a week without their knowledge. This would be directed surveillance and because it is a local authority, will require the authority of a magistrate.*



## Module 2: Working as a CCTV operator

### Chapter 4: CCTV and relevant legislation

**The Protection of Freedoms Act 2012** creates the post of a **Surveillance Camera Commissioner** who now has the role of encouraging compliance with the code of practice which was discussed in chapter 3. This code applies only to relevant authorities although the Commissioner would like all CCTV systems to adopt the 12 guiding principles of the code. These 12 guiding principles are also set out in chapter 3.



#### CCTV evidence

When a criminal court, civil court or tribunal considers a case, it will hear the evidence from witnesses. Evidence can be presented in a number of different ways and an understanding of the principles might assist the CCTV operator to produce good quality evidence.

Evidence can be presented in the following ways:

- **Testimony** – witnesses stand in court and give a verbal account of the event – CCTV operators giving evidence about the actions they took concerning an incident.
- **Real evidence** – any material object introduced in a trial, intended to prove a fact, often made up of exhibits.
- **Exhibits** – items that are connected to the case, e.g. CCTV DVDs, weapons used in an assault.
- **Documentary evidence** – any evidence introduced at a trial in the form of documents. Although this term is most widely understood to mean writings on paper (such as a contract), the term actually includes any media by which information can be preserved. Photographs, tape recordings, films and printed emails are all forms of documentary evidence. Therefore DVDs would be considered as documentary evidence.
- **Circumstantial evidence** – a series of facts, when taken together, suggest that the person is guilty, but on their own do not conclusively prove guilt.
- **Primary evidence** – the original copies of DVDs, CDs, etc. and secondary evidence will be copies. Producing the original evidence will always be preferable in court.

The important principle for **criminal courts** to prove is that the evidence should show, '*beyond reasonable doubt*', that the defendant(s) are guilty. This means that if the defence can create reasonable doubt in the eyes of the court, the defendant will be acquitted.

In a **civil court**, the proof will depend on something known as the '*balance of probabilities*' which means the court will consider 'was it likely to have happened rather than not' before finding guilt. The onus is on the claimant to prove their case not the defence.

**Tribunals** usually sit as a panel, incorporating a legally qualified tribunal chairman, as well as panel members with specific areas of expertise. They hear evidence from witnesses but decide the case themselves. Tribunals have limited powers (depending on the jurisdiction of the case) to impose fines and penalties or to award compensation and costs. A tribunal will generally follow the civil court principle of finding guilt on the balance of probabilities.

## Module 2: Working as a CCTV operator

### Chapter 4: CCTV and relevant legislation

The main impact of the Surveillance Camera Commissioner Code is to ensure CCTV is used for a legitimate reason and pressing need, and that there is public confidence in the way in which it is used.

When directed surveillance has been properly authorised, there will be a time limit attached to the authority, currently a maximum of a three-month period, it can be renewed. Before it has been authorised, the proper forms must be completed and approved by the appropriate person. If the police are authorising, an officer not below the rank of superintendent can authorise for pre-planned surveillance. In urgent cases a police inspector may authorise verbally, but it has to be confirmed in writing as soon as possible afterwards and it will only last for 72 hours.

When directed surveillance is required by a local authority, it must be authorised by a magistrate and there are some limitations to the reasons it may be approved. Covert surveillance may also be carried out by other agencies, including the security services, Revenue and Customs. Each agency will have a specific level of senior officer who may authorise the surveillance.

The reasons for authorising directed surveillance are also shown above, but if any of these reasons cease to exist, then surveillance must cease straight away.

CCTV operators who are asked to carry out surveillance by the police or other agencies should always ask them (if not sure) whether the request falls under RIPA legislation or not. If authority is required, it is essential that it should be obtained or confirmed if the images are to be accepted in a court. Unauthorised directed surveillance is unlikely to be allowed in court as evidence.

#### **The Police and Criminal Evidence Act 1984 (PACE)** (PACE is not applicable in Scotland).

This act sets out a number of issues concerning evidence and impacts on CCTV by ensuring evidence is treated correctly. If CCTV evidence has been obtained or treated unfairly or if there is no audit trail, for example, PACE may cause it to be excluded from being used in court.

The following process should be followed when CCTV evidence is being produced for court:

- Incident recorded by the operator;
- Incident log and any other notes completed;
- Police attend (may wish to view incident) and request DVD/CD etc. (formal request);
- Two copies produced:
  - 1) **master copy** - placed in secure storage.
  - 2) **working copy** - handed to police officer or other agency and signed for; and
- Statement written by operator for police file to include brief outline of incident on view, all actions by operator and copying process if done by same operator as well as exhibiting the CDs/DVDs. Statement writing is covered in more detail in chapter 8.

To preserve the integrity of any DVD/CD, etc. its progress and location should be controlled by way of an audit trail. This is essentially a written record of who has handled the evidence before the court and where it has been stored. Access to a master copy must be controlled and restricted to prevent allegations of the evidence being tampered with. CDs/DVDs should be held in secure bags with numbered seals to preserve the audit trail.

#### **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 to pursue all reasonable lines of enquiry to obtain relevant evidence. The impact on the CCTV operator is that the police may wish to access a large amount of CCTV recording, including images not of a particular incident, but from adjacent cameras, and that process can be lengthy. The police may also wish to retain written notes and logs if they deem them to form part of the investigation. Note that it is the responsibility of the police (or other agency) to disclose CCTV evidence to the defence, not the CCTV operator, whose role will merely be providing that evidence to the police or other agency.

## Module 2: Working as a CCTV operator

### Chapter 4: CCTV and relevant legislation



#### Scotland

The Police and Criminal Evidence Act 1984 (PACE) and the Criminal Procedure and Investigations Act 1996 (CPIA) does not exist in Scotland. However, the relevant legislation is covered under Schedule 8 (8) of the Criminal Procedure (Scotland) Act 1995.

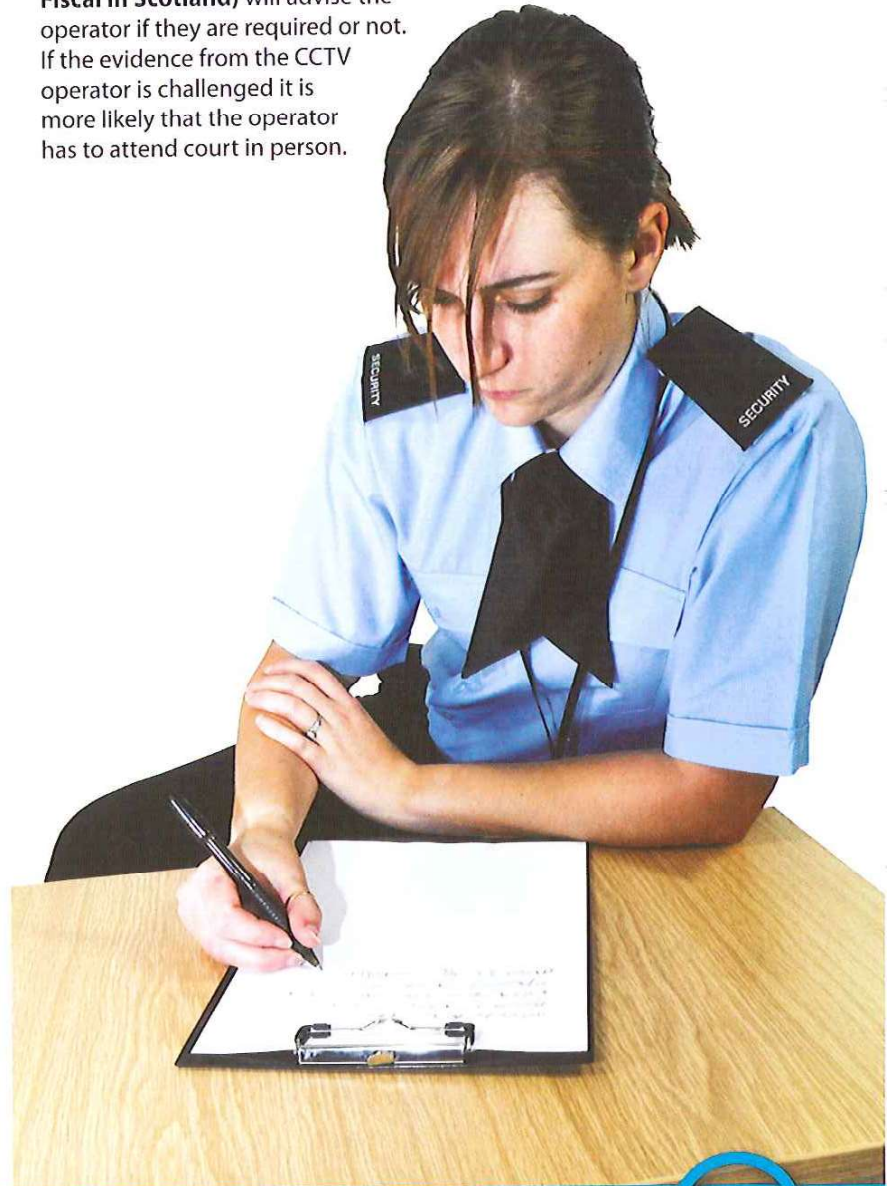
Under this piece of legislation it clearly identifies that:

- A 'document' includes, in addition to a written document, any film, negative, tape, disc or other device in which one or more visual images are recorded so as to be capable of being produced as evidence;
- With regards to the recovery of documents it is the legal right of the sheriff court to make, in connection with any criminal proceedings, an order for the recovery of any document by a Justice of the Peace Court, sheriff solemn or summary, or the High Court;
- The Criminal Justice and Licensing (Scotland) Act 2010 (CJLSA) controls how evidence is gathered and introduces codes of practice that will help prove that evidence was gathered lawfully. Section 116 of the act gives the police the power to seize evidence, including evidence contained on computer;
- The collection of evidence from a CCTV system should adhere to an agreed procedure. This is commonly declared into the code of practice from the ICO; and
- The CJLSA controls the gathering of evidence, and directs the police and the Crown as to what evidence must be disclosed to the defence prior to the court hearing. This is known as 'disclosure'.

#### CCTV operator statements

When a court case is likely, the CCTV operator will have to produce a statement detailing their actions. Chapter 8 explains the content of such a statement, but operators must be aware of the importance of providing such a document. If a statement is completed, good practice is to retain a copy for future use. Each statement will have a declaration by the writer that it will contain the truth and that any deliberate falsehood could be an offence.

If the CCTV operator's evidence is not challenged by the defence, the statement written by them may be accepted and the operator may not need to attend court. The Crown Prosecution Service (**Procurator Fiscal in Scotland**) will advise the operator if they are required or not. If the evidence from the CCTV operator is challenged it is more likely that the operator has to attend court in person.



## Module 2: Working as a CCTV operator

### Chapter 4: CCTV and relevant legislation

There are two types of court room a CCTV operator is likely to have to attend. The **magistrates' court** and the **Crown court**.

A magistrates' court is a smaller court with two or three magistrates sitting in judgement. The clerk to the court acts as a legal adviser to the magistrates, who are normally drawn from local people of good character.

The **prosecution** is represented by a lawyer from the Crown Prosecution Service and they will ask questions and put the case for the prosecution. The **defence** is represented (usually) by a lawyer who will challenge the evidence and question witnesses in order to disprove the case. In some cases the defendant may choose to represent themselves in court, but this is unusual. The magistrates' courts tend to deal with less serious offences but in some circumstances can send a case to the Crown court to be tried.

The Crown court is a larger court, dealing with more serious cases and the chairman of a Crown court is normally a judge or recorder. The evidence is heard before a jury who are made up of members of the population chosen beforehand. The operator will still have to give evidence in the same way as at a magistrates' court.



**SCO**

**Justice of the Peace courts:** A Justice of the Peace is a lay magistrate, appointed from within the local community and trained in criminal law and procedure. Justices sit either alone, or on a bench of three, and deal with the less serious summary crimes, such as speeding, careless driving and breach of the peace. In court, justices have access to advice on the law and procedure from lawyers, who fulfil the role of legal advisers or clerk of court.

**Sheriff courts:** The majority of cases are dealt with in the country's sheriff courts unless they are of sufficient seriousness to go to the supreme courts at first instance.

There are six sheriffdoms in Scotland. Each sheriffdom has a sheriff principal charged with a number of duties in respect of the courts for which they are responsible, including in particular a duty 'to secure the efficient disposal of business in the sheriff courts of that sheriffdom'.

Criminal cases are heard by a sheriff and a jury (solemn procedure), but can be heard by a sheriff alone (summary procedure).

**The High Court of Justiciary** is Scotland's supreme criminal court. When sitting at first instance as a trial court, it hears the most serious criminal cases, such as murder and rape. A single judge hears cases with a jury of 15 people.

Cases in the high court are prosecuted by Advocate Deputes. They are advocates or solicitor-advocates who are appointed by the Lord Advocate, in whose name all prosecutions are brought in the public interest. It is possible, although extremely rare, for a private prosecution to be brought.

Tribunals are often run like a court room, but less formally and with less powers (see tribunals).

## Module 2: Working as a CCTV operator

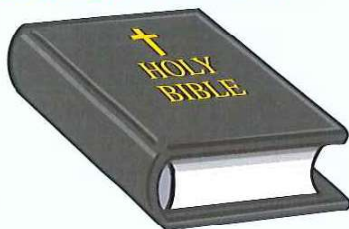
### Chapter 4: CCTV and relevant legislation

#### Attending court

Before attending court, the operator should take the opportunity to refresh their memory by reading their statement. Attending court can be a stressful experience and the courts have a witness support system that can assist with the process of operators preparing themselves before giving evidence in court. The following sets out what can be expected:

- Arrive at court in good time and let CPS know you are the CCTV operator witness;
- Read your statement (if not already read through);
- When called into court, stand in the witness box. If you have a faith, you will be asked to take an oath. If Christian, you will have to hold a Bible and read the oath:

*'I swear by almighty God that the evidence I give, shall be the truth, the whole truth and nothing but the truth.';*



- There are different books for each religion, for example, the Koran for Islam, but if the witness does not wish to take an oath, (they may be agnostic) they can take an affirmation as follows:

*'I do solemnly, sincerely and truly declare and affirm that the evidence I shall give shall be the truth, the whole truth and nothing but the truth.';*



- You will be asked questions by the solicitors (barristers in the Crown court), but you should address your answers to the magistrate or jury as it is they who will consider your evidence;
- Try and keep your answers straightforward and avoid trying to embellish your statement. If you do not know the answer to a question don't be afraid to say so; and
- Avoid giving opinion (unless asked) or making assumptions; your job is to report the facts of what you saw and did.



## Module 2: Working as a CCTV operator

### Chapter 4: CCTV and relevant legislation



#### Sexual offences legislation

We have mentioned the need for operators to avoid viewing subjects that could be classed as inappropriate or by intruding unlawfully into private areas.

The **Sexual Offences Act 2003** and the **Sexual Offences (Scotland) Act 2009** creates the offence of voyeurism which establishes the following crime:

*'The observation (for the purpose of sexual gratification) of another person doing a private act, knowing that the person did not consent to being observed.'*

This could actually be committed even if cameras are not used, but there is also a linked offence which covers the use of equipment, including CCTV, to carry out the basic offence. It is a criminal offence and offenders can be imprisoned if they are convicted.

The immediate impact upon CCTV operations is that operators must justify their use of CCTV at all times, and particularly when images of a sexual nature are viewed. In many public space systems, it is quite possible that persons will carry out sexual activity in view of the cameras. If operators are to continue viewing these, they should consider the following criteria:

- Is an offence being committed by the person(s) involved?  
For example, is a man threatening a woman with a knife?
- Does each person appear to be consenting to the activity?  
Are there signs of a struggle? and
- Is there any evidence that someone is drunk or drugged?  
Are there signs of uncontrolled actions or obvious drunken behaviour?

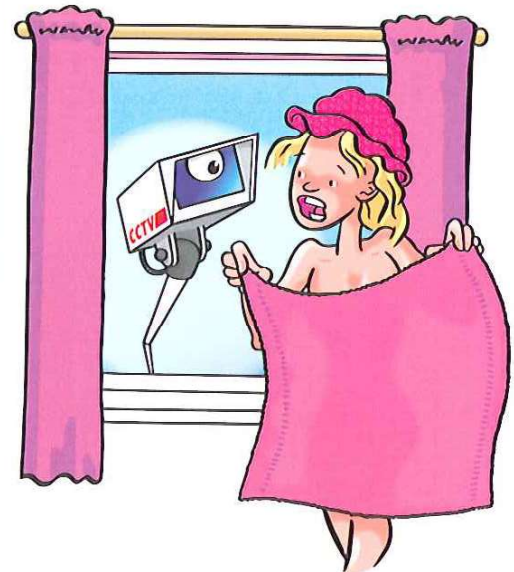


If none of the listed criteria is evident the operator should zoom back from the scene. However, it should be remembered that what might start out as consensual may change and monitoring from a wider view may be appropriate.

Other considerations in respect of sexual activity is to be aware of where and when it takes place. Persons doing so late at night in a remote area may not require action whereas persons in a public car park during the day, perhaps when shoppers are around, will require action.

Persons will be deemed to be doing a **private act**, if they are in a place which, in the circumstances, would reasonably be expected to provide privacy for example: a bedroom, bathroom, changing room etc. and:

- a) The person's genitals, buttocks or breasts are exposed or covered only with underwear.
- b) The person is using a toilet.
- c) The person is doing a sexual act, not of a kind ordinarily done in public.



## Module 2: Working as a CCTV operator

### Chapter 4: CCTV and relevant legislation

#### Child exploitation

The Sexual Offences Act 2003 and the Sexual Offences (Scotland) Act 2009 and the Sexual Offences (Northern Ireland) Act 2008 also created offences of arranging or facilitating child sex offences and CCTV operators should be aware of the possibility that public space cameras may view incidents when children are being groomed or developed for such offences. Grooming is the process by which an offender draws a victim into a sexual relationship and maintains that relationship in secrecy. The following indicators may be visible by way of CCTV and effective operators should familiarise themselves with them.

Indicators of child exploitation include:

- Older non-intoxicated men escorting children and young people who are intoxicated;
- Children/young people in the company of older people or anti-social groups;
- Young people acting in an inappropriate and sexualised way with adults or older people;
- Children developing expensive new habits with alcohol or drugs abuse;
- Uncharacteristic behaviour changes;
- Showing fear in certain company;
- Having cuts and bruises from assaults; and
- Wearing unaffordable new clothes or having expensive phones.

Visible warning signs of children being trafficked:

- Young people checking into accommodation with older men;
- Children and young people arriving and departing from a location with different adults on the same day or over a period of time; and
- Children and young people getting into and out of a number of different cars.

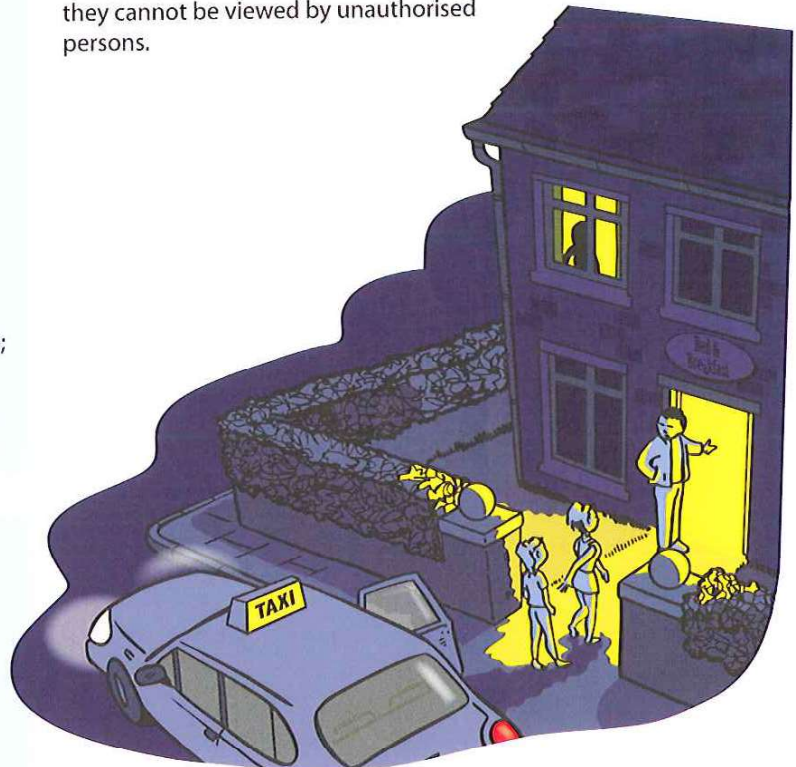
#### The sex offenders register

The sex offenders register contains the details of any individual convicted, cautioned or released from prison for a sexual offence against children or adults since 1997.

It is quite possible that CCTV operators could be requested to monitor persons who are known to be sex offenders, either by an authorised partner (e.g. the police) or by personally knowing the person concerned.

In these cases, the operator should always check before carrying out the monitoring, firstly whether a RIPA authority is required or not and secondly, is the monitoring proportionate and reasonable, given the circumstances.

In any case where sex offenders' images are being processed, it is essential that confidentiality is maintained to a high standard. When images are on view in the control room, operators must ensure that they cannot be viewed by unauthorised persons.



## Key Task 4

- 1 Write down in the space below 3 areas which, in your opinion, are NOT allowed to be viewed by CCTV cameras during the day-to-day use of a CCTV system:

1

2

3

- 2 Give 3 examples of behaviour that could suggest a child or young person is at risk:

1

2

3

- 3 Give 2 reasons that might allow someone's privacy to be ignored with CCTV cameras:

1

2



## Module 2: Working as a CCTV operator

### Chapter 5: Communications within CCTV operations

#### CCTV and communications

CCTV control rooms will almost certainly have some method of communication with other agencies or departments. A town centre system may well have a radio link with shop managers, and in some control rooms, a police radio link or connection to traffic enforcement staff may exist.

Whilst an incident is taking place, CCTV operators may well have to be in touch with persons at the scene or other emergency services, for example police, fire, ambulance coastguard. The information a CCTV operator provides could assist any of the agencies to manage and deal with incidents more effectively. For example, persons being sought by the police can be searched for, tracked and followed by CCTV with the location being passed to the officers looking for them.

One of the primary uses for CCTV is to help provide safety and security with cameras assisting in the management of areas with crowds, for example shopping centres, sports arenas or travel hubs. Monitoring crowd movement by CCTV can help prevent overcrowding and ensure people's safe passage.

Effective CCTV operators also make good use of CCTV to collect information about active criminals and pass that information to enforcement agencies. The police and other enforcement agencies rely heavily on the information passed to them not only by the public, but also from CCTV operators who can gather images of active criminals for use by the intelligence departments.

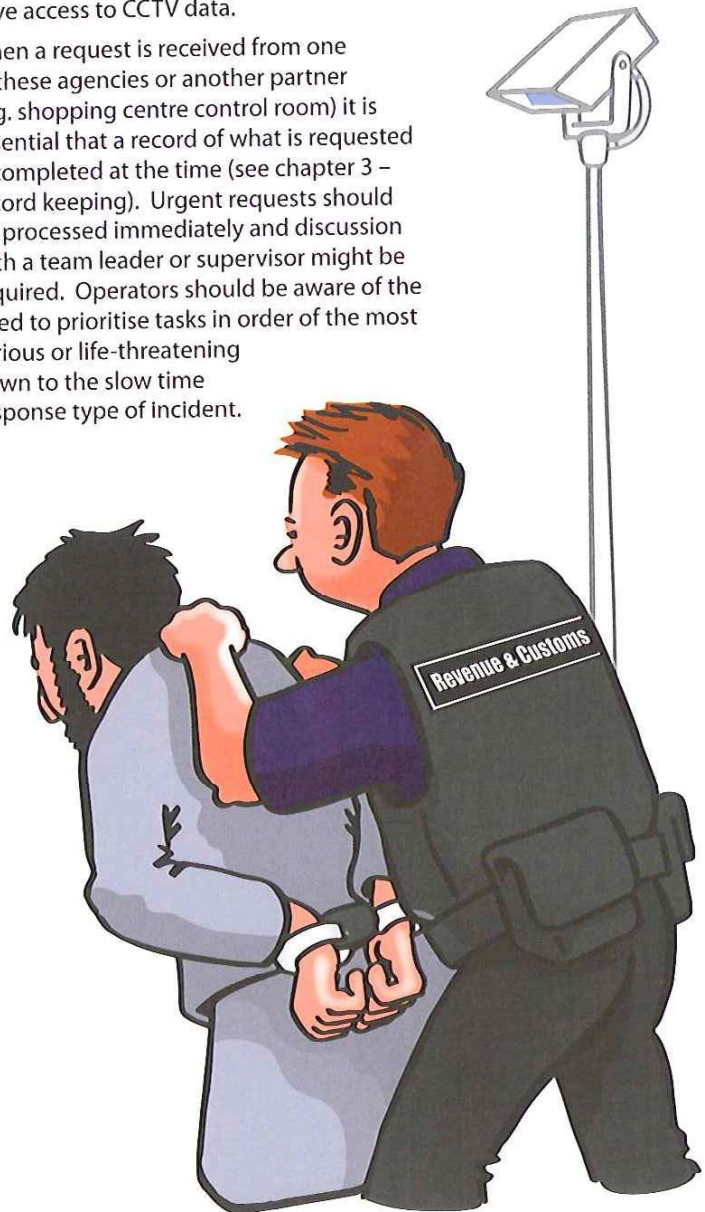
Even though there may be a radio link in the control room, some town centre CCTV systems have a dedicated person from the other agency in attendance to assist with operational effectiveness. For example, some of the larger CCTV control rooms have a police officer assigned at busy periods to assist in management of the area covered by the cameras.

#### Enforcement agencies

From time to time CCTV control room staff will work with other enforcement agency personnel who have enforcement abilities, for example the police, Border Force officers, Revenue and Customs officers, Health and Safety Executives.

Other smaller organisations are usually part of police operations, for example the National Crime Agency and the Serious Fraud Office (government department with investigation and prosecution powers). There may be other official partners to CCTV staff who are involved in the day-to-day running of the control room and who may have access to CCTV data.

When a request is received from one of these agencies or another partner (e.g. shopping centre control room) it is essential that a record of what is requested is completed at the time (see chapter 3 – record keeping). Urgent requests should be processed immediately and discussion with a team leader or supervisor might be required. Operators should be aware of the need to prioritise tasks in order of the most serious or life-threatening down to the slow time response type of incident.



## Module 2: Working as a CCTV operator

### Chapter 5: Communications within CCTV operations

#### Working as part of a team

There are a number of reasons why having an effective team and working closely together can benefit CCTV operations.



### The benefits of working as a team

(Figure 7)

Operators should have a proactive approach to working with other members of the team as the following benefits can be achieved:

Benefit	How it can be achieved
Increases efficiency by sharing workloads	Colleagues could be setting up cameras when the operator is tracking persons ahead of a camera change, they can be contacting the police when the operator is trying to follow a suspect at speed, etc.
Allows each person to work to their individual strength and ability	Some operators might have better surveillance skills and can react quicker to developing situations.
It helps to focus operators on common targets	Everyone can concentrate on a particular task, making it more likely to be completed successfully and there is no duplication of tasks.
Improves the communication between team and partners	If everyone has the same information it saves time, and messages do not get confused, there is no duplication of time, critical information or tasks.

Many incidents witnessed by CCTV operators take place in 'fast time' and having access to resources to attend, whether it is a police officer, security guard or other partner (police community support officers, traffic enforcement officers, etc.) can make all the difference to the successful outcome of the incident. Having a dedicated communication link speeds up this process and ensures that the information goes to the right person at the right time.

Some town centre CCTV control rooms have a secure police radio installed under licence and this gives them direct contact with police control rooms or the officers on patrol. These systems are usually encrypted and are treated as secure access for privacy. There may also be a radio system linking the shops in a town centre allowing immediate contact to shop staff to warn of suspects or for them to contact the control room with descriptions of offenders for circulation and monitoring. One important factor to remember is that shop staff may not be as skilled as control room staff and their radio technique might not be as effective.

Operators will have to use their skill and judgement when dealing with untrained radio users.

It is highly important that any communication, whether on the radio, telephone or by any other method, is carried out in an accurate and timely manner. Any delay in the passing of a description to others may result in that suspect being lost or emergency services not attending quickly enough to detain them. Evidence and potential witnesses at the scene may also be lost as a result.

Where there is a local reporting procedure or process in place, it should be clearly followed as the effectiveness of it might depend on accuracy and timeliness.

In serious incidents, police supervisors, managers and other senior staff will need to have all the facts of an event in their possession before making decisions. The CCTV operator may be key to that process and must always be professional in their approach to communication standards.

A graphic featuring a dark grey key shape with a white circle at the end of its shaft, positioned over a blue circle. The text "Key Task 5" is written in white on the dark grey key.

## Key Task 5

- 1** The Data Protection Act 2018 sets out principles. *What might principles 5 and 6 deal with in relation to CCTV data?*

- 2** The Human Rights Act sets out a number of articles. *What do articles 8 and 14 relate to in respect of CCTV?*

- 3** Voyeurism is an offence under the Sexual Offences Act. *What is specifically not allowed to be viewed according to the legislation?*

## Module 2: Working as a CCTV operator

### Chapter 6: Emergencies and CCTV

IEDs can be delivered in four ways:

- Unattended objects;
- Vehicle carried;
- Person-borne; and
- Postal.

#### Emergency procedures involving CCTV

We live in a world where terrorism is a risk to every person. There is a national security threat level issued by the security services, and operators should always be aware of the threat level in place at that time. CCTV has a primary function of helping to provide safety and security for us all. Operators should be proactive with CCTV at all times, remaining vigilant when on duty, but never more than when the security risk is high.

Any item can contain an Improvised Explosive Device (IED) and it is the circumstances surrounding the item that will allow the operator to decide whether there is a need to explore further.

**Unattended objects** – in deciding if they are suspicious the operator should consider their type and location. IEDs can be very small and it is difficult, if not impossible, to say if a small package contains explosives or not. Indicators of IEDs inside packages may include the following:

- Items with wires protruding or batteries visible;
- Packages left in high profile locations;
- Backpacks or luggage that is out of place; and
- Items that appear weighted down.



## IED?

**Vehicles** that carry IEDs are difficult to identify as there are vast numbers of vehicles moving in and out of our towns and cities all the time. Operators should be aware of possible locations where a vehicle-borne IED could be left, for example:

- Buildings with a high profile occupant, e.g. government buildings;
- Areas where there are large numbers of people and vehicle access;
- Sports grounds; and
- Shopping centre car parks.

The list is endless and each location should be considered as a risk in its own right by the operator.

Indicators for suspicious vehicles will include:

- Vehicles left in unusual places, perhaps with hazard lights displayed;
- Wires coming from the vehicle; and
- Vehicle is very low on its suspension.

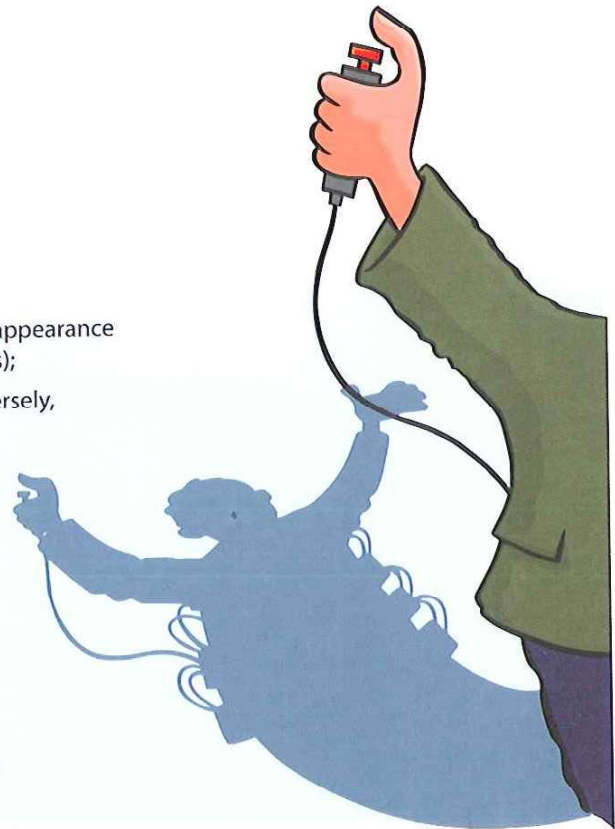


## Module 2: Working as a CCTV operator

### Chapter 6: Emergencies and CCTV

**Person-borne IEDs** (suicide bombers) are difficult to identify and are usually directed in highly populated areas full of tourists or people enjoying entertainment, e.g. sports grounds. The following indicators might suggest person-borne IEDs:

- Clothing is out of sync with weather, location, or suspect's appearance (e.g. long coat in hot weather, loose clothing to hide bulges);
- Displays excessive sweating, mumbling, fidgeting, or conversely, being unusually calm and detached;
- Eyes are focused/appears to be in a trance;
- Hands are kept in pockets;
- Pats upper body as if checking something;
- Has pale face from recent shaving;
- Walks deliberately, does not run;
- Exhibits an unnatural gait and posture;
- Unresponsive to commands, salutations; and
- Hands and arms may have chemical burns/bleaching from handling or mixing chemicals to make explosives.



**Postal IEDs** may not just contain explosive material, but could also have dangerous biological or chemical contents designed to injure or incapacitate. CCTV operators may not be the first person handling a postal package, but obvious signs that there could be a risk include the following.

#### Obvious signs:

- No return address;
- Misspelt words;
- Marked as personal;
- Sealed with tape;
- Stained or emitting a strange odour or powder;
- Excessive packing tape; and
- Unexpected parcel.



The principle of treating any unexpected package as suspicious is a good one and local procedures should be in place to deal with anything believed to be a security package risk. This will also apply to suspicious packages found in the CCTV control room.



## Module 2: Working as a CCTV operator

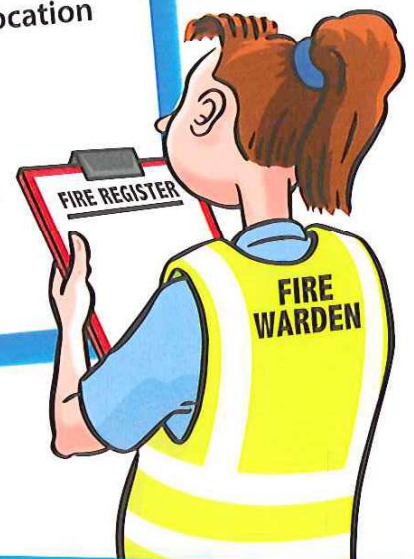
### Chapter 6: Emergencies and CCTV

#### Evacuation of the CCTV control room

When the decision has been taken to evacuate a CCTV control room, there is likely to be a local procedure in place. Evacuation may be for different reasons, and might require different procedures, for example

a fire would require a slightly different procedure to a suspect package. If there is a procedure in place, it should be followed but the following steps *might* also be included as part of that procedure and will assist in the smooth evacuation process:

- Confirm emergency services have been contacted;
- CCTV systems should remain on and have images transferred to any other control room (where this is possible);
- Mobile phone or radio communications should be taken (when possible) with evacuating staff;
- Personal items (if nearby) may be removed by the staff but only if it does not delay the evacuation process; this might also reduce the number of objects to be searched in a control room;
- The control room should be made secure, but access keys (for emergency services to use if required) and control logs taken out;
- Windows closed (where possible) and internal doors might be left open and lights left on, unless evacuation is caused by fire when all should be closed;
- All staff should go to the designated assembly point, unless that would place them in more danger when an alternative assembly point should be used or a location specified by the emergency services; and
- The last person to leave should confirm there is no one else in the control room. This might be a fire marshal's responsibility in cases of fire.



## Module 2: Working as a CCTV operator

### Chapter 6: Emergencies and CCTV

#### Searching the CCTV control room

Some CCTV control rooms are so small that searching could be carried out in a very short period of time, whilst the larger control rooms might need more than one person to search. In either case the search is best carried out by someone who knows the layout and what should normally be there.

It is likely that staff in the CCTV control room will be aware of items that do not belong, for example cardboard boxes or unfamiliar bags.

It is good practice to question anything unfamiliar when seen at the start of a shift, to allay any suspicions as to its origin. When a search has to be undertaken, do so in a methodical way. If anything is found that cannot be accounted for, ask if it belongs to a member of staff.

Almost anything could be disguised as an IED and we have previously described what could be classed as a suspicious item. If an item found in the control room continues to be unexplained, a supervisor should be informed and evacuation should be implemented without delay. In any case, CCTV operators should be familiar with their local procedure in how to deal with suspicious items in the control room. It is never a good idea to assume that an item is not capable of causing harm.

In reality, anything could be treated as suspicious and it will depend on the circumstances surrounding it being found in the control room. If anything is found that cannot genuinely be accounted for, the following should apply:

- Do not touch it or try to move it outside;
- Do not put water on it;
- Contact the police or supervisor – preferably by landline, but avoid using a radio in close proximity;
- Warn others to vacate the area;
- Make a mental note of the item, or take a picture with a mobile phone if one is available; and
- Consider the fact that it may have a biological, radioactive or chemical element and use the local procedure to implement further action.

#### Reoccupying the CCTV control room

When the evacuation has been resolved and staff can go back into the control room (ensure emergency services have agreed) there are a number of procedures to follow:

- Equipment should be checked as per the normal functional checks process (discussed in chapter 8);
- Ensure the operator log has been updated with details of the evacuation reasons etc.; and
- If required, scan recorded images for events taking place whilst the control room was unmanned.



## Key Task 6

- 1 What indicators might a CCTV operator look for to determine whether someone is about to place a suspicious item in a town centre?

- 2 State 3 actions to take when evacuating a CCTV control room:

- 1
- 2
- 3

- 3 If a suspicious package is found either outside or inside the control room, what advice about the item should be followed?



## Module 2: Working as a CCTV operator

### Chapter 7: The impact of health and safety on CCTV

#### CCTV operations and health and safety

In many CCTV control rooms the operator will be working alone, particularly at night, so it is important that their health and safety is taken into account. There are a number of methods by which this can be effectively carried out:

- Regular check calls from other control rooms or supervisors;
- Visits by other staff or supervisors; and
- Electronic devices to confirm they are alive and well – when no activity has been detected other staff elsewhere are made aware.

Check calls (telephone or radio) identify the immediate state of the operator's health and safety and are considered the most effective method of checking on staff.

#### Display screens




CCTV control rooms all contain equipment that operators have to view (monitors) or manually control (keyboards, computer mouse). Health and safety law sets out how staff should make use of such equipment under the Health and Safety (Display Screen Equipment) Regulations 1992.

There is a requirement upon employers to carry out a workstation **risk assessment** for each member operating such equipment on a consistent regular basis. This assessment will include the setting up of each workstation on an individual need as staff will all have different criteria to make themselves comfortable at a workstation (different heights, different eye standards, individual chair set-up, etc.).

In order to ensure the regulations are met, the operators should be given some training in how to set up their workstation to comply with the regulations. The employer should also ensure that operators are given the opportunity to have regular breaks away from the screen. This effectively means not viewing any screen during that break, usually about 10 minutes per hour, when operators have *constantly* been viewing monitors. This is usually achieved by a change of task or more naturally when operators have to make notes or take phone calls etc.



The following might be included in a workstation risk assessment:

-  Display screen set-up – brightness, contrast, angle of display, etc.;
-  Desk set-up – position of screens, height of desk, distance from screen(s);
-  Keyboard/control – is the keyboard or control unit suitable for the individual?
-  Chair set-up – height, rake, arm position, neck support, etc.;
-  Environment – room temperature, lighting (reflections), space, noise, etc.; and
-  Individual – does the operator need glasses for screens? Do they have access to a wrist rest or mouse mat?

## Module 2: Working as a CCTV operator

### Chapter 7: The impact of health and safety on CCTV

#### Managing stress

It is fair to say that all types of work attract their own levels of stress, both physical and emotional and it is essential that CCTV operators recognise when stress becomes a problem for themselves or colleagues.

Work-related stress places a responsibility upon the employer to deal with it in some appropriate way to help the member of staff being affected. This responsibility includes minimising the risk of stress-related illness or injury to employees.

Of course there may be non-work related stress affecting the member of staff and this should be taken into account by the employer in dealing with them, although there is also an onus placed on the member of staff to take reasonable care of their own health and safety and others who may be affected by their actions.

Stress can manifest itself in the following ways:

#### Physical symptoms of stress include:

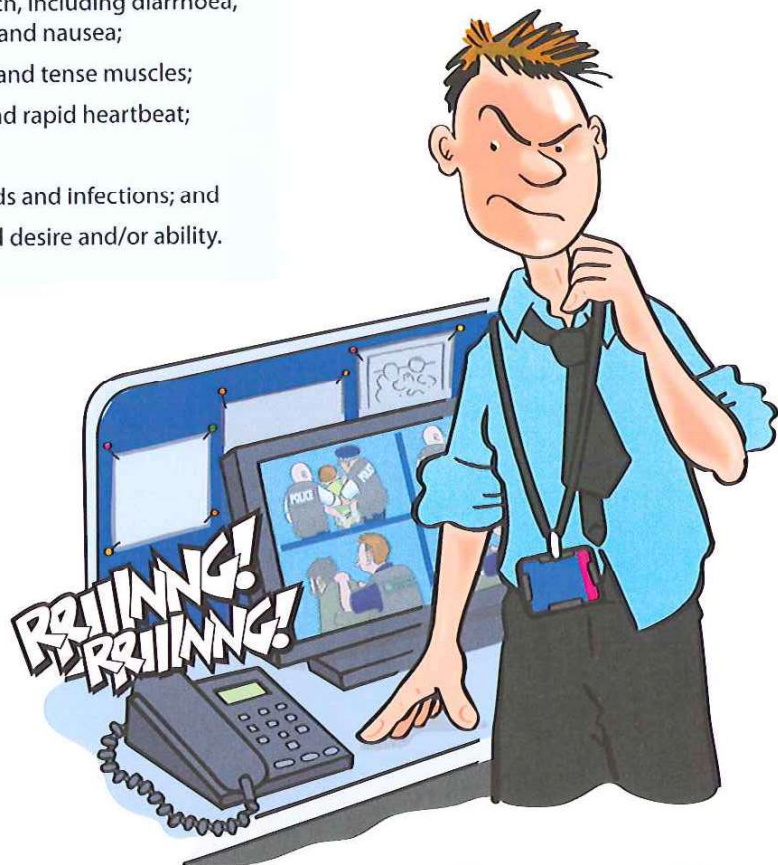
- Low energy;
- Headaches;
- Upset stomach, including diarrhoea, constipation and nausea;
- Aches, pains and tense muscles;
- Chest pain and rapid heartbeat;
- Insomnia;
- Frequent colds and infections; and
- Loss of sexual desire and/or ability.

#### Emotional symptoms of stress include:

- Becoming easily agitated, frustrated and moody;
- Feeling overwhelmed, like you are losing control or need to take control;
- Having difficulty relaxing and calming your mind;
- Feeling bad about yourself (low self-esteem), lonely, worthless and depressed; and
- Avoiding others.

#### Cognitive symptoms (mental abilities) of stress include:

- Constant worrying;
- Racing thoughts;
- Forgetfulness and disorganisation;
- Inability to focus;
- Poor judgement; and
- Being pessimistic or seeing only the negative side.



## Module 2: Working as a CCTV operator

### Chapter 7: The impact of health and safety on CCTV

**Behavioural symptoms** of stress include:

- Changes in appetite - either not eating or eating too much;
- Procrastinating and avoiding responsibilities;
- Increased use of alcohol, drugs or cigarettes; and
- Exhibiting more nervous behaviours, such as nail biting, fidgeting and pacing.

Alleviating work-related stress should be undertaken with the assistance of the employer, who has a responsibility to take reasonable steps to minimise the risks of stress. Possible avenues of relief could include some or all of the following:

- Communicate with others - a friend or your GP or work supervisor;
- Take a step back, detach yourself and look at the situation from another angle;
- Improve your diet - eat more healthily;
- Take regular exercise - walk around the control room;
- Explore various methods of relaxation - yoga, meditation, massage, walking, fresh air;



- Progressively tense and relax muscles: legs, stomach, back, shoulders, neck; and
- Exercise your toes: curl them against the soles of your feet as hard as possible.

#### Risk assessing

We have explored the need to carry out a risk assessment for health and safety reasons, but this applies to the daily working of a CCTV operator in other areas. The overall reason for a risk assessment is to find hazards and minimise them. The workplace can be an area where risks are present and never more so than in a CCTV control room which will have electrical equipment and other hazards present.

The onus is on all of us to be aware of the risks that may be present in the workplace and elsewhere to help provide safety and security for ourselves, work colleagues and the public at large. Employers are required to carry out a workplace risk assessment for employees and others, but it is not necessary to be a health and safety expert in order to carry out a risk assessment and employers often undertake this with a designated member of staff or external consultant.

There are five stages to a risk assessment – how it might affect operators is shown as well:

- Identify the hazards – CCTV operators view areas where there may be serious hazards present: a hole in the road, a broken kerb and risk of fire, etc.;
- Decide who might be harmed and how: the public, work colleagues, visitors, etc.;
- Evaluate the risks and decide on precautions: informing other agencies, contacting other staff, maintenance, etc.;
- Record your significant findings: make a note in the operator log, maintenance log, accident book etc.; and
- Review your assessment and update if necessary: monitor if there has been any change in the risk.

CCTV operators should remember that a primary aim of CCTV is to provide a safer environment for the general public and so identifying hazards outside of the control room is just as important as those inside. Any non-action is likely to attract an enquiry or even litigation when an identified hazard which has not been corrected has resulted in serious injury or death. Operators may very well identify a hazard in the public domain and these should be reported to the appropriate authority for action. For example, a hole appearing in a pavement should be reported to the local authority for action.



#### Hazards and risks

- A hazard is anything that may cause harm, such as chemicals, electricity, trip hazards, working from ladders, an open drawer; and
- The risk is the chance, high or low, that somebody could be harmed by these and other hazards, together with an indication of how serious the harm could be.

A graphic consisting of a dark grey speech bubble with a white circle inside, containing the text 'Key Task 7', and a blue circle with a white speech bubble shape inside it, partially overlapping the first one.

- 1 What items could be adjusted when setting up for operators according to the display screen regulations?

- 2 If a CCTV worker is alone in a control room, give some examples of how a supervisor could check on their welfare:

- 3 What are 3 symptoms an operator might suffer if they were affected by stress?

1

2

3

- 4 Give 3 examples of a hazard that might be found in a CCTV control room:

1

2

3

## Module 2: Working as a CCTV operator

### Chapter 8: Practical use of CCTV

#### Practical use of CCTV

##### Suspicious activity

What is suspicious to one person may not be to another. It will depend on the circumstances surrounding the surveillance. If the actions seen on the monitor could be described as dubious, distrustful, apprehensive or unsure then it should be treated as suspicious. One important fact to remember is that when the operator has the belief or impression that someone is involved in illegal or dishonest activity, it is always preferable to take action rather than ignore what is seen. It is better to respond even if the suspect's activity turns out to be lawful.

When something suspicious is seen, make sure the cameras are used as quickly and effectively as possible:

- If the system does not record all the time, ensure recording is started immediately;
- Get close-up views of persons. Remember, if someone starts to run, keeping them in view when zoomed in is much harder to achieve, so once the close-up has been obtained, pull back to a suitable view. The recording will now have a close-up of the suspect to refer to;
- Try and get adjacent cameras adjusted to pick up the suspect when moving (if you have colleagues in the control room, they may be able to assist in this way); and
- If the area viewed is sizeable, allow the camera to give sufficient viewing area for an investigator to interpret what is on the screen.

In any surveillance where the image size identifies a person or persons, CCTV operators must take into account the implications of the Human Rights Act and the right to respect for a person's private life. The overriding principle is that when the view is likely to be evidential an operator should be able to justify the surveillance.

In chapter 3 we show the size of images that can be obtained depending on the requirements at the time of the event.

##### Multiple incidents

Working as part of a team can be challenging. It is essential that you develop a good working relationship with others in the CCTV team to be properly effective and professional. Figure 7 chapter 5 sets out the benefits of having the assistance of other members of the team. The decisions being taken by all concerned can have a legally binding impact on the subjects being viewed by cameras. For example, if you pass information to the police that a suspect is present and they arrest that person on your say so, then your actions must be professional and of the highest standard. If your decision-making is good, the police and other agencies are more likely to take notice of the information you pass them.

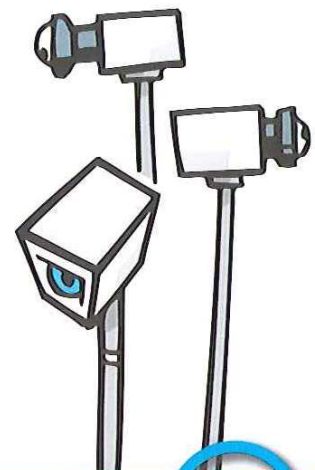
Contacting external agencies and other partners during an incident is a normal part of CCTV operations. Your ability to communicate well is likely to determine the effectiveness of the interaction with these partners. The use of radios will be examined later in this chapter but you should make use of the phonetic alphabet and ensure messages have been received by the recipient correctly.

Written work must be of a high standard and is often the first impression others will get of your ability to communicate and your professionalism. Reports written clearly and concisely will assist your colleagues and managers to process the information contained within.

During an emergency or urgent incident, events may move quickly and CCTV operators will take notes about what they see and what they have been told by others. These notes are usually written in a desk notepad or other notebook used at the desk. These are known as the operator's **original notes** and may be required for evidential purposes. This is because information written down at the time it is received or shortly afterwards is more likely to be accurate than trying to remember something for days or weeks past. These notes should be retained by the operator in case they are required by an investigator at a later stage.

When a control room is busy, more than one incident may be taking place. CCTV operators must be able to decide which event has priority. The decision should be taken on the following criteria:

- **Risk to life** – is the event life-threatening requiring immediate action?
- **Risk of serious injury** – will persons be seriously injured as a result of no action being taken?
- **Loss of evidence** – if no action is taken will evidence be lost or destroyed, or will suspected persons escape?
- **Risk of damage to property** – if no action is taken will damage be caused to property?



## Module 2: Working as a CCTV operator

### Chapter 8: Practical use of CCTV

#### Body language traits

Body language is most commonly defined as **non-verbal communication**. CCTV operators cannot hear what is being said by persons in the street and so have to rely on what is seen. Developing and improving your skill in identifying body language traits will make you more effective.

The following list is by no means exhaustive but is intended to help operators and supervisors give some thought to the body language that they are constantly monitoring as part of their role. These will all depend on the circumstances of what is taking place at the time and will not apply to all circumstances generally.

### Body language and its meanings

(Figure 8)

From the following list, consider just how many expressions of body language you actually recognise – you'll be surprised!

Body language	Meaning
Brisk, erect walk	Confidence
Standing with hands on hips	Readiness, aggression, frustration
Sitting, legs apart	Open, relaxed
Arms crossed on chest	Defensiveness
Walking with hands in pockets, shoulders hunched	Dejection
Hand to head contact – general	Heightened stress
Hand to cheek, rubbing chin	Evaluation, thinking
Touching, slightly rubbing nose	Rejection, doubt, lying
Rubbing the eye	Doubt, disbelief
Hands clasped behind back	Anger, frustration, apprehension
Locked ankles	Apprehension
Head resting in hand, eyes downcast	Boredom
Rubbing hands	Anticipation
Sitting with hands clasped behind head, legs crossed	Confidence, superiority
Open palm	Sincerity, openness, innocence
Palms facing down	Calming signal, passive
Pinching bridge of nose, eyes closed	Negative evaluation
Tapping or drumming fingers	Impatience
Patting, fondling hair	Lack of self-confidence, insecurity ( <i>may be preening or trying to arouse interest</i> )
Tilted head	Interest
Stroking chin	Trying to make a decision
Looking down, face turned away	Disbelief
Biting nails	Insecurity, nervousness
Pulling or tugging at ear	Indecision

## Module 2: Working as a CCTV operator

### Chapter 8: Practical use of CCTV

Watching persons moving around is a normal part of the CCTV operator's role and identifying suspicious behaviour is a skill that can be developed. If someone is testing the effectiveness of CCTV they may move around whilst watching the cameras to see if they are being tracked or followed.

Operators may see someone trying to conceal items and avoid being seen by cameras. These all add to the level of suspicion an operator develops for the view on screen.

When watching groups of people, for example during the night-time in a town centre, it can be difficult to see what behaviour is taking place. CCTV operators should make good use of cameras to zoom in and monitor behaviour closely. Obvious body language displays can include pushing and shoving and people standing close to each other, face to face. This is often a sign of conflict.



#### Operating CCTV

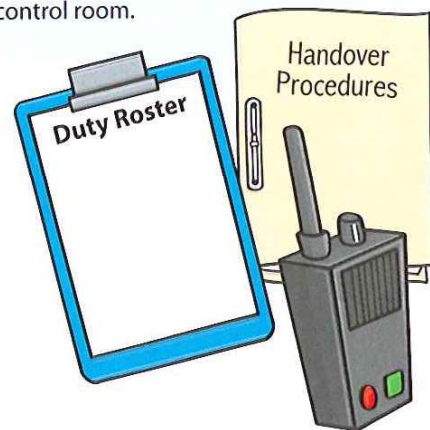
Handover procedures are essential if the incoming CCTV operator is to get up to speed with current and proposed events. If there are emergency incidents in progress, the outgoing operator will either have to remain working on the incident or pass enough information to the incoming operator so that the incident can be handed over correctly.

Functional checks are the routine system checks carried out at the start of each shift by the operator to ensure that the system is working correctly. It is an essential part of daily routine and each time a fault or problem is identified, it should be reported according to the local procedure.

Checking should be at the start of a shift or duty and should be methodical and systematically completed with any forms being completed accordingly.

The routine to be followed by the operator includes the following, but there may be other things to check depending on local requirements:

- A handover routine should be completed with the outgoing operator;
- A radio check should be carried out;
- Desk and seating should be arranged by the operator to meet health and safety rules. Paperwork and desk is set up ready for operational use;
- Equipment including cameras, monitors and control panels are all working correctly;
- Recording of images should be confirmed (if access to recording is available);
- Alarm systems should be functioning correctly; and
- Computers and other ancillary equipment used in the day-to-day running of the control room.



## Module 2: Working as a CCTV operator

### Chapter 8: Practical use of CCTV



#### Fault reporting

When a fault has been found (possibly when functional checks have been done) the person finding should report it using the agreed procedure. This is usually going to require the completion of a suitable fault reporting form.



(Figure 9)

### Example fault reporting form

Below is an example of the type of form likely to be completed:

FOR COMPLETION BY CCTV OPERATOR				FOR COMPLETION BY ENGINEER		
John Smith				Roger Blake		
FAULT IDENTIFICATION				ROUTINE SERVICE AND REMEDIAL WORK		
TIME	DATE	OPERATOR	FAULT (INCLUDE CAMERA NO)	TIME	DATE	ENGINEER
1400	13/10/14	J Smith	Camera 6 intermittent fault. Goes blank every 10 seconds.	1200hrs	14/10/14	RB
FAULT REPORTING				DETAILS OF WORK CARRIED OUT		
TIME	DATE	OPERATOR	RESPONSE			
1500	13/10/14	J Smith	Passed to engineer; they will deal asap.	0900 14/10/14 Camera inspected – new power unit fitted by engineer. Tested and fully functional.		



## Module 2: Working as a CCTV operator

### Chapter 8: Practical use of CCTV

A key issue here is that each time the fault is found, a new form or update should be completed.

This will allow the manager to monitor the overall maintenance of the system and any recurring fault might require additional action by engineers.

From a health and safety aspect, if engineers are working (possibly at height) on a system, the operator should be made aware they are working to ensure that equipment is not operated which might affect the engineers well-being.

Operators should be able to make good use of keypads and/or joysticks as a matter of routine. This aspect of practical use is essential if they are to get the best possible pictures from their system.

Most keypads have buttons to select monitors and cameras, and operators should familiarise themselves as quickly as possible when first starting to operate keypads.

Joysticks are the most common form of control to move PTZ (Pan, Tilt and Zoom) cameras and allow the operator to keep viewing the screen whilst moving the camera. This is not always the case, with PTZ cameras being moved by a computer mouse or by using up and down controls on a computer keyboard.

Whilst most CCTV operators complete written incident logs and records, many now use computer programmes to complete the process and operators may need to understand these programmes in order to do so.

#### Reports and statements

The need to complete clear and accurate reports and statements is an essential part of a CCTV operator's role. Often, these reports and statements will be part of the evidence in a court case and they will have to be set out in a clear but concise fashion, only including the relevant information. A CCTV operator will complete incident logs for events that are significant and these can be written to suit the operator but still need to include the relevant information (See figure 3).

Incident logs should be completed as soon as the information is available. Remember, notes (descriptions) written at the time or soon afterwards are more likely to be accurate and accepted by a court. Relevant information will include the following:

- Descriptions of persons should include their gender, ethnicity, height (sometimes difficult because cameras are high up) clothing and other features;
- Vehicle descriptions should include make and type, colour and if possible a registration number, which would be the most important aspect of a vehicle. (Some vehicles have false number plates, but still record the number displayed.); and
- The event can be described also. Keep the detail clear and brief and avoid making assumptions but include information such as the direction of travel of persons or vehicles, what they did, any injuries suffered, if known, details of security officers or police attending.



## Module 2: Working as a CCTV operator

### Chapter 8: Practical use of CCTV

This is an example of a written police statement of a fictitious incident which contains the relevant information for a court case. The statement would be made by referring to the notes and incident log made by the operator at the time or soon after the event.

The statement will contain a declaration that the writer is telling the truth and could be prosecuted for knowingly making untrue statements:



This statement consisting of 1 page(s) is true to the best of my knowledge and belief and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have wilfully stated in it anything that I know to be false or do not believe to be true.

Signed: John Smith 13/10/14

I am a CCTV operator working for Headshire Borough Council in their CCTV control room. I hold an SIA licence for CCTV number 123456. The cameras cover the town of Headshire and I have control over the ones that have a moveable function. All images are recorded by way of a digital recording system.

At 1100hrs on Monday 13th October 2014, I was on duty in the control room, when my attention was drawn to a man standing in the High Street, Headshire near to the Post Office. I would describe him as male, about 35 years old, white, about 5ft 10 inches tall. He was wearing a blue denim shirt, dark trousers and white trainers. He had short dark hair, was clean shaven and was not wearing glasses. As I watched him on camera 6 he walked along the pavement towards the Marks and Spencer shop, up to an elderly female and I saw him push her in the back, whilst at the same time grab her handbag from her right hand. She fell into the doorway and the man made off, running across the road through traffic, into an alleyway which leads to the town centre car park. I followed him using camera 6 and then to camera 8. My colleague immediately contacted the police and I was able to maintain contact using CCTV. He ran to a small white Ford van and I saw that the registration was RO 06 E2K. He entered the van and drove towards the High Street exit. As he entered the High Street a police vehicle caused him to stop and two officers went to the driver, who was the same person I had seen take the handbag. There was no one else in the vehicle. He was detained by the police officers and I saw them remove the handbag from the front passenger seat of the car. The entire CCTV coverage was recorded by the system.

At 1200hrs the same day, I interrogated the system and made two copies of the entire event onto two blank read only DVDs. The first copy had the unique reference number of 131014/345 and I am producing this as exhibit JS/1. This was placed in the secure evidence store. The second copy was made onto a blank read only DVD with the unique reference number 131014/346 and I am producing this as exhibit JS/2. I completed the appropriate forms covering the copying process. At 1230 hrs the same day, PC 1144 Middleton came to the CCTV control room and I handed him the working copy marked with the unique reference number 131014/346 which he signed for upon receipt. At the time of the incident, the CCTV system was working correctly.

Signed John Smith

Statements can vary considerably, depending on the amount of information available. CCTV operators need to keep them clear and concise and only include facts. The process of making copies of the images needs to form part of the statement, but this is often carried out by other operators and therefore they would need to complete a statement covering their part in the process and to prove an audit trail.

Later in this study book are some example forms for students to complete. You may either make up a fictitious event or make use of the Internet and use some video of an incident to complete the forms and compile a police statement.

## Module 2: Working as a CCTV operator

### Chapter 8: Practical use of CCTV

#### Tracking suspects

Following a person on foot or a vehicle at speed takes practice. A car or person moving quickly will soon be out of camera view if the camera is zoomed in too closely. This might seem contrary to getting a good clear close-up of a suspect for evidential purposes but the operator should ideally try and get both views. Keeping someone or a vehicle in view will almost always require the use of other cameras and the effective operator will have an adjacent camera set up to view the subject as they move out of range of the other camera.

If the subject appears to be moving out of the system area, then (depending on the reason for surveillance) informing the next CCTV area (if any) would be appropriate. If passing the subject's location to the police or other partners is required, then details should be recorded in the operator log.

Watching people moving around is a normal part of day-to-day CCTV activity. When persons enter or leave an area, keeping them in view requires a good knowledge of the area and what cameras are in place. When someone appears to be deliberately trying to avoid cameras, getting a close-up image will be difficult. The operator must always consider why they might be trying to avoid being seen and should remember that they could be involved in or about to commence some illegal activity.

When a subject has been lost, the operator should set up cameras to cover as many doors, alleyways, etc. as possible. Start with the last location the subject was seen and search in that area first, working around in a 360 degree pattern. Arrange other adjacent cameras to cover nearby and if available, get the assistance of colleagues.

Use a methodical and systematic search pattern and if the search continues for a long time, note down what areas have been searched and advise colleagues, particularly if you are ending a shift and a new operator is coming on duty (this is more relevant for suspect items).

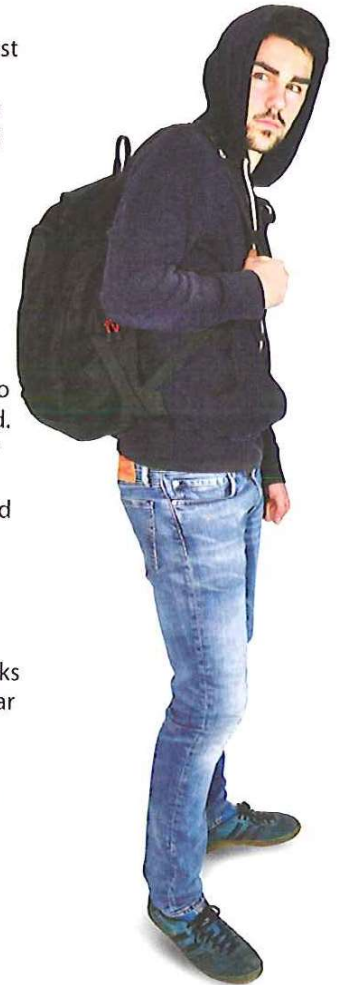
#### Suspicious persons/items

If the CCTV control room receives a request to search for suspicious people or item(s) the information given to operators is very important. Details about a person should start with the gender and clothing worn and then go on to the other descriptive information. A CCTV operator is likely to see the clothing of a person at a distance, before anything else about them.

A suspicious package could be anything small or large and fine detail is essential, so making use of any PTZ cameras is required. Items connected with criminal activity, for example discarded stolen goods, should have close-up images obtained (400%) and a note made in the log as to the location. Speedy communication with the police or other agency might also be required to prevent their loss.

Searching the outside of buildings, car parks and outside areas in general requires a clear system of searching in order to cover all the visible areas thoroughly. In a car park, work along each line of parked cars, trying to obtain vehicle registration numbers if possible for use by investigators at a later stage if required. Make a note of where you have searched (as above, for other operators).

There will be areas that are not visible by cameras and there is little that can be done to cover these unless there are security officers etc. on the ground to assist in the search.



**When you compile your written police statement consider using the person shown above as the example for describing persons.**



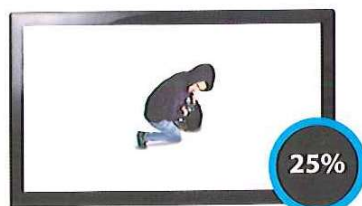
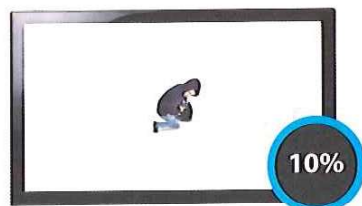
## Module 2: Working as a CCTV operator

### Chapter 8: Practical use of CCTV

#### Producing CCTV evidence

One of the most important roles a CCTV operator may have to undertake is the production of CCTV images for use as evidence in court. For any evidence to be accepted in a court, certain procedures must be followed and operators **must** be aware of these procedures. A flow chart of this process is shown later in this chapter.

For images to be accepted as good quality evidence they first have to be of a suitable size and we have set out the Home Office advice here:



#### Monitor - 5% Screen Height

The general view on the screen when a CCTV operator wishes to monitor a wider area to watch people's behaviour.

#### Detection - 10% Screen Height

This will be achieved by capturing the image of a person, which occupies at least 10% of picture screen height on the monitor and is often used where the CCTV pictures are being monitored live. The operator is not concerned about what the person looks like as security guards will or may be deployed to apprehend the intruder.

#### Observation - 25% Screen Height

This will be achieved by capturing the image of a person, which occupies at least 25% of picture screen height on the monitor. This is often used to observe a group of people such as in a town centre and understand what they are doing. Once this has been established the operator should, if necessary, take appropriate action.

#### Recognition of a known person - 50% Screen Height

This will be achieved by capturing the image of a person, which occupies at least 50% of picture screen height on the monitor. On a CCTV system this is the minimum size that the police are likely to use in a court case to recognise a person within the picture.

#### Identification of an unknown person - 100% Screen Height

This will be achieved by capturing the image of a person, which occupies at least 100% of picture screen height on the monitor. This is most often used at doorways to give an excellent high-quality picture of people passing through. It is normally required by the police at the entrances to licensed premises.

#### Inspection of an item or object - 400% Screen Height

This is the view that may be obtained when inspecting a suspicious package or trying to identify writing on an object without sending security staff, police or bomb disposal to inspect the object.

This view is valuable because it can prevent putting staff at risk by allowing a CCTV operator to view an object 'up close', but from a safe distance.

## Module 2: Working as a CCTV operator

### Chapter 8: Practical use of CCTV

When an incident is likely to result in evidential images, the following stages are typical in the production of images:

- Incident recorded – the images are recorded into the system by an operator;
- Request from agency – police, for example, may request officially a copy or just come and ask to view the images. If they view only, this process must be recorded in a suitable log record. If they ask for a copy, an official request is usually accompanied by a completed request form, according to local procedure. (Some police forces have their own forms.);
- Copies made by an operator (not always the same one) – one master, one working;
- Both copies will be issued with a Unique Reference Number (URN) from a register in the CCTV control room. (No two copies will have the same URN number.);
- Master copy should go to a secure evidence store in a sealed evidence bag or similar;
- Working copy handed to agency – such as the police, **upon signature** with URN and usually with a statement of evidence from the operator recording the event **and** the operator copying the discs (as this may be a different operator);
- Exhibit label completed (police usually provide these) and handed over with disc. The exhibit number is made up of the person exhibiting using their initials and a number. For example, John Smith's first disc (master copy) will be exhibit JS/1; and
- Any other paperwork provided to the police. This may be incident log, rough notes, etc. Some systems make use of pro-forma statements to assist operators.

It is essential that when evidence is handed over from the operator to the police and then from one police officer to another one, a signature is completed on the handover

record. This process creates what is known as an **audit trail** and shows that the evidence has been correctly processed and removes allegations of evidence tampering. The police or other agency is responsible for any defence lawyers having access to video evidence.

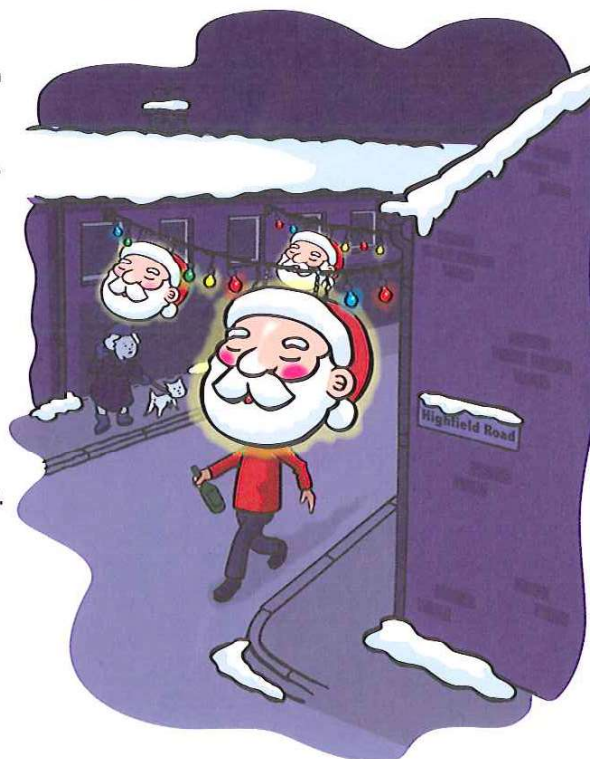


#### Environmental considerations

Producing clear CCTV images requires good lighting, clear weather and efficient equipment. When poor weather, for example fog or heavy rain, prevents good quality images there is little that can be done to improve them. However, lighting can be used to good effect when there is a low level of natural light. There are different types of lighting available and cameras tend to prefer strong lighting in order to process images. However, in complete darkness the use of infrared lighting is desirable. In chapter 2 infrared lighting was discussed as high frequency lighting that the human eye cannot see, other than the red light bulb/LED glow of the actual light producing the infrared frequency. This type of lighting allows a camera (which is responsive to infrared) to see in the dark. The infrared light is reflected back into the camera lens and gives a monochrome image.

CCTV operators will get to know the area each camera can view, and becoming familiar with each camera's limit of operating is essential for effective operation. In some cases, the camera can be limited by being in the wrong position or when building work has obstructed the camera view. There can also be temporary obstructions such as scaffolding, Christmas decorations or advertising banners in the street blocking the camera view. If other cameras are available on the system, the operator should make the best use of them.

Some cameras have screen wipers for operation in the rain. These are activated by the operator from the control room and often have a water spray facility as well.



**1** What sort of information would be included in a police statement?

**2** When using CCTV cameras, what size of image would allow for 'inspection' of a person or item, for example a suspicious package?

**3** Give 3 examples of body language signals that would suggest a person is angry:

**1**

**2**

**3**