GET
LICENSED

# CCTV OPERATOR TRAINING
# STUDY NOTES

**Level 2 Award**

For CCTV Operators in the Private Security Industry

Dear Student,

Greetings and welcome to the CCTV Operator training. Please read the following information carefully.

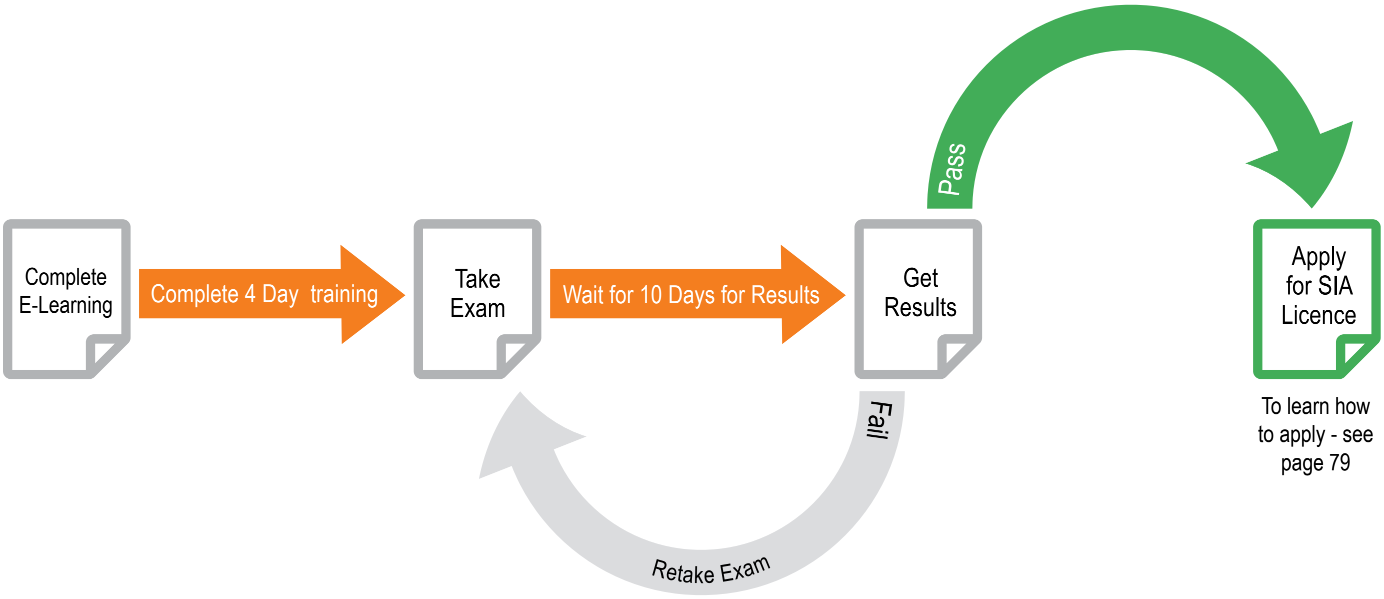
The CCTV Operator course has **two units as well as Practical Assessments** and runs over **three** days.

**Remember:**

1. You must attend all three days of training.
2. Bring the relevant ID Documents on the exam day.
3. Complete your pre-course e-learning module.
4. Participate actively in the training process.

**Key Information** (Please complete and retain for your records)

| | |
|---|---|
| **Training Provider Name** | |
| **Instructor Name** | |
| **Exam Date** | |
| **Expected Results Date** | |



To learn how to apply - see page 79

## FAQ

### Q. When is the exam?

A. The exams are on the last day of the course.

### Q. How long will it take to get the results?

A. Results are sent via email and SMS message as soon as the exam body marks them. Please allow ten working days from the date of your exam to get your results.

### Q. When can I apply for the SIA Licence?

A. You can apply for the SIA Licence once you have received your result and you have passed all four units.

### Q. What if I fail my exam?

A. In the unlikely event of failing one or more units, you will have to come to retake the exam(s). The current exam retake fee is £90, if you have the Flexi+ package, you can take unlimited exam retakes at no extra cost. If you are worried about your exams and would like to upgrade to Flexi+ -- please speak with your instructor.

### Q. What if I am not happy with the course?

A. If you are unhappy with any aspect of your course, first speak with your Instructor, if you are not happy with the outcome, please inform Get Licensed, and we will **do the right thing!**

**Your success is our success!**

## CCTV Operator Exams and Assessments

Course Duration: Classroom of 22 Hours taught over 3 Days:

| Exam Name | Number of Questions | Pass Mark | Time Allowed |
|---|---|---|---|
| **Principles of Working in the Private Security industry** | 72 | 51 (70%) | 1 Hour 50 Min |
| **Principles of Working as a CCTV Operator** | 40 | 28 (70%) | 1 Hour |
| **Various CCTV Practical Assessments including:**<br>Use of Radios<br>Report Writing<br>Use of CCTV Equipment | NA | NA | NA |

**Mock Exams - scan to take a mock exam.**

# Identity documents required for SIA courses

☑ One identity document from the list Group A **and**

☑ Two documents from the list Group B **and**

☑ A passport size photo of yourself

!

**Out of the three documents, at least one document must show your current address and at least one document must show your date of birth. Each document should be the original, physical document. The SIA will not accept a scan or photocopy.**

## Group A documents list

A1 Current, valid UK passport.

A2 Current, valid passport of any other nationality.

A3 Current, valid photocard driving licence if it was issued by the DVLA in Great Britain.

A4 Current, valid photocard driving licence and its paper counterpart issued by the DVA in Northern Ireland.

A5 UK original birth certificate issued within 12 months of birth.

A6 Current, valid UK biometric residence permit card.

## Group B documents list

B1 Bank or building society statement issued to your current address, less than three months old. You can use more than one statement as long as each is issued by a different bank or building society.

B2 Utility bill (gas, electric, telephone, water, satellite, cable) issued to your current address within the last three months. You can only submit one utility bill in support of your application.

B3 A credit card statement sent to your current address within the last three months. You can submit more than one statement as long as each is issued by a different issuer.

B4 Council Tax statement issued in the last 12 months.

B5 Mortgage statement issued in the last 12 months.

B6 Letter from H.M. Revenue & Customs, Department of Work and Pensions, employment service, or local authority issued within the last three months. You can submit more than one letter as long as each is issued by a different Government department or a different local authority.

B7 P45 statement of income for tax purposes on leaving a job issued in the last 12 months.

B8 P60 annual statement of income for tax purposes issued in the last 12 months.

B9 Current UK driving licence - paper version (not the paper counterpart to a photocard).

B10 Driving licence photocard (without a paper counterpart) issued by the DVA in Northern Ireland.

B11 Pension, endowment or ISA statement issued in last 12 months.

B12 Valid UK firearms licence with photo.

**First Aid Requirement for Door Supervisor and Security Officer training**

You must complete the First Aid qualification as part of your training package unless you already have a current and valid First Aid or Emergency First Aid certificate which you must bring on your course (your certificate must be valid for at least 12 months from the start date of your security course).

# Table of Contents

**Unit 1: Principles of Working in the Private Security Industry ... 7**

Chapter 1: The Characteristics and Purposes of the Private Security Industry ... 8

Chapter 2: Legislation awareness ... 17

Chapter 3: Arrest Procedures ... 27

Chapter 4: Health and Safety ... 32

Chapter 5: Fire Awareness ... 39

Chapter 6: Emergencies ... 43

Chapter 7: Communication ... 51

Chapter 8: Record Keeping ... 56

Chapter 9: Terror threats and the role of the Security Operator ... 63

Chapter 10: Keeping Vulnerable People Safe ... 72

Chapter 11: Post incident Management ... 77

**Unit 2. Principles Of Working As A CCTV Operator In The PRIVATE SECURITY INDUSTRY ... 78**

Chapter 1: The Purpose of CCTV and The Roles and Responsibilities of a CCTV Operator ... 79

Chapter 2: The Impact Of Legislation On CCTV Operations ... 83

Chapter 3: Operational Procedures in Public Space Surveillance ... 93

Chapter 4: CCTV Equipment ... 98

Chapter 5: Surveillance Techniques ... 103

Chapter 6: Different Types of Incidents and how to respond to them ... 107

Chapter 7: Health and Safety in The CCTV Environment ... 109

PRACTICAL USE OF CCTV EQUIPMENT ... 112

ADDITIONAL RESOURCES ... 116

BECOME CERTIFIED SECURITY PROFESSIONAL ... 117

# PRINCIPLES OF WORKING IN THE **PRIVATE SECURITY INDUSTRY**

# CHAPTER 1 The Characteristics and Purposes of the Private Security Industry

**Security:** Protection of a person, building or organisation against threats such as crime.

**Need for a private security industry:** In today's world, the private security sector works hand in hand with the police and government organisations to help protect the public.

**Security is provided in 3 ways:**

1. **Manned security** - people on-site looking after its security
2. **Physical security** - locks, gates and barriers
3. **System security** - CCTV, alarms etc

**The purpose of the private security industry is to:**

- Prevent and reduce loss, waste and damage
- Monitor and respond to safety risks
- Provide personnel (Door Supervisors, CCTV operators, Security officers)
- Provide security systems for people, property and premises

**The Private security industry act 2001:**

This law was passed through Parliament in May 2001 and came into force in 2003. Its main aim was to set, maintain and raise standards in the UK's private security industry. In order to enforce and manage the new law, the government formed a new body called the Security Industry Authority.

Part of the SIA's main aim is to protect the public and licence people working in certain sectors within the UK's private security industry.

**Security Industry Authority:**

- Reports to the government
- An independent body set up to enforce regulation of the private security industry.
- Reduce criminality and raise standards within the private security industry
- Empowered by the Private Security Industry Act 2001

- Compulsory licensing of individuals
- Voluntary Approved contractor scheme set up for security companies.

**In order to receive an SIA licence the candidate must meet the following criteria:**

- Must be a minimum of 18 years old
- Must attend and pass a regulated course in the sector for which they want to work eg: Door Supervisor Course, Security Officer Course, CCTV operator course etc.
- Must have the right to work in the UK
- Must not have been convicted of certain offenses or have certain unspent offences in the past 5 years as stipulated under the Act

Anyone working in the below private security sectors must be trained and licensed by the **Security Industry Authority (SIA).**

- Door Supervisor
- Security Officer
- CCTV operator
- Cash and Values in Transit (CVIT)
- Close Protection
- Keyholding
- Vehicle immobilisation (only in Northern Ireland)

The SIA are required to keep records of the following information:

- Licence number
- First and last name
- Activity (e.g. Door Supervisor, Security officer etc.)
- Role (front line, non-front line)
- Licence expiry date
- Licence status (active, expired, revoked)
- Date licence status changed.

**Licence Linked Qualifications Expanded:**

**Door Supervisor** - Carries out duties at licensed premises where alcohol is consumed on-site.

**CCTV (Public space surveillance)** - Monitor the activities of the public or private place

**Security Officer** - Providing security services in various types of retail or corporate premises.

**CVIT** - Guarding cash or valuables and transporting them between banks and companies

**Close Protection** - Guarding one or more individuals against assault suffered in consequence of the actions of others.

**Key Holding** - Taking custody of keys for buildings or premises and responding to alarm call-outs, there is no Key Holding licence. However, any key holder is required to hold some form of SIA licence (Door Supervision or Security Officer)

**Vehicle Immobiliser** - Only valid in Northern Ireland, restrict vehicles using a device and demand payment for release.

**Key Bodies:**

- **SIA** - Security Industry Authority, an independent body, reports to the government
- **NSI** - National security inspectorate
- **BSIA** - British Security industry association
- **Local Authorities** - Councils etc
- **Police** - private security help support the police
- **Other security associations** - there are a number of these in the sector.
- **Skills for Security** - help to raise standards.
- **British Standards** - UK's national standards body

**SIA Code of behaviour:**

The SIA has set a strict code of conduct that all licensed individuals as well as approved contractors are required to follow:

- Act fairly and reasonably without discrimination
- Use clear language
- Perform duties in a courteous and professional manner
- Display integrity and understanding

**The Required Standards of Behaviour of Security Operatives:**

All Security operatives are expected to have the following qualities:

- Be Reliable - Come to work on time and always do their duties to the best of their abilities
- Have Integrity - Being honest and have good morals
- Be Polite - A large part of security’s role is customer service
- Professionalism - Look smart and well dressed
- Responsible - be prepared to take responsibility for your actions
- Be well dressed and look presentable while on duty

**Key Skills:**

- Be a good clear communicator with colleagues, management and customers
- Always check understanding
- Remember that communication is always 2 way, both parties should understand one another
- You are part of a team, always work within your strengths within the team
- Some situations the security may be sensitive in nature so a security operative should be mindful of this and handle these in a sensible manner

Security staff should always adhere to both the SIA standards of behaviour as well as their own company’s standards and values

**Crime reduction initiatives** - Local authorities help set up partnerships to help reduce crime, for example, Pub/Club Watch, partnerships with local police and radio link schemes where all pubs and clubs are linked via radio.

**Police Liaison Officers:**

These partnerships also could involve police liaison officers who will work directly with venues to help share information and help reduce crime. Monthly/weekly briefings can be held with businesses in the area to share information and update them of current issues in the local area.

**Red Card/Yellow Card Scheme:**

This scheme is used for Licensed Premises (Businesses that sell alcohol to the public) that have ongoing problems, it's a way to give a business a chance to make improvements as opposed to just closing a business down for failing to comply with the law when it comes to the sale of alcohol (more on this later)

**Yellow card:** Business given the opportunity to improve, perhaps given stricter conditions in which they will need to operate

**Red Card:** Business is shut and their licence is revoked

The idea of the card system is not to punish potentially innocent members of staff who would lose their livelihoods if the business is closed. Also other businesses could suffer as a result of the closure such as nearby food establishments etc

**Removing the opportunity for crime to take place:**

- Improve lighting in the area
- Improve the physical security (locks, barriers etc)
- Install CCTV cameras
- Control access to the site
- Cooperation with Police as well as the local authorities
- Liaising with other venues in the area via radio link schemes and sharing of information of issues in the area, for example sharing information about someone who is banned from your site with other sites nearby

**Assignment Instructions (AI's):**

These are security operative's set of guidelines as to what they need to do on any particular site that they are working on, they can differ from site to site and will be designed by both the security company and the company that they are providing security for. They are a contract between the security operative and their employer.

They help make sure that security operatives are:

- Following the law
- Maintaining company policies
- Complying with client instructions

Types of activities covered:

- Search procedures
- Site plans
- Duty times
- Areas of vulnerability
- Health and safety procedures
- Important telephone numbers
- Alarm procedures
- Emergency procedures
- Day to day operations
- Communication methods (radio, telephone, written)
- Access and egress control procedures
- Number of patrols and how these should be carried out
- Need to be signed and understood by security officers

Security Operatives need to make sure that they read and understand their AI's before they start work on a site. AI's are also confidential documents so should not be shared with any unauthorised individuals.

**The Use of CCTV within security:**

**Benefits of using CCTV:**

- Crime prevention - clearly visible cameras can deter criminals
- Detect Crime - provide clear images of crimes being committed to be used as evidence in investigations and trials
- Safety - providing an overview on an environment which allows for hazards to be spotted and measures taken to reduce the risk to the public and employees
- Traffic management - can be used to monitor traffic on motorways etc
- Access control - identification of visitors to a site
- Reduction of staff required (reduction in operational costs) as CCTV can cover large areas quickly
- Recorded Images can be used in investigations
- Recorded images can be used as evidence in prosecutions in courts of law

**Legal implications of using CCTV:**

- Any public space surveillance CCTV system must be registered with the **Information Commissioner's Office** (ICO)
- The data controller (owner of the CCTV system who must be named) has a legal responsibility for any data processed through the CCTV system
- There must be adequate signage to inform the public that cameras are in operation and these signs must also contain contact information for the data controller so that members of the public can raise complaints or issues
- CCTV systems cannot record in certain areas which would be deemed as private such as toilets/changing rooms etc
- Collecting of any personal data including images that are identifiable are protected under the Data Protection Act 2018
- Any information that comes into a CCTV operator's possession falls into this category.
- Any disclosure of any information must be authorised
- Responsibility to disclose or not is placed on the person being requested for information

- If the operator is unsure they should seek clarity from their supervisor/team leader
- Access to control rooms must be controlled
- Only authorised trained individuals should be allowed access to the data recorded

Any 3rd party security operative working within a CCTV control room will require an SIA CCTV licence

**Limitations of CCTV systems:**

- The general public may feel that CCTV infringes their privacy, as a result of this certain areas can not have cameras in operation
- The system is always vulnerable to damage as well as vandalism that may be costly to repair
- There is a risk that the system is misused by members of staff which could incur anything from a loss of job in less serious situations to a loss of licence or even criminal proceedings in more serious situations
- Although CCTV is a good deterrent to crime it cannot prevent crime from happening, in some cases an operator may be a witness to a crime and not be able to physically do anything about it at the time
- While in the long term the CCTV system can save on costs, the initial outlay to install the equipment and train the staff may be quite expensive
- Cameras do also have view limitations, there may be areas that just aren’t covered by the system

**CCTV Technological Vulnerability:**

- Any moving parts in the system (Pan, Tilt, Zoom) will have a tendency to wear out over time and will need to be replaced
- Lenses can get a build up of dirt and will need to be periodically cleaned
- Sunlight can cause the images to be hard to see
- Weather can also cause interference with the system
- Although technology is moving quickly forward (facial recognition etc), systems still need operators to be effective

- Transmission methods can be compromised through damage to wiring
- Low light environments will require infrared cameras to be effective

**The SIA Approved contractor scheme:**

The approved contractor scheme is designed to help the SIA raise standards within the private security industry and assist the private security industry in developing new opportunities. The SIA do this by placing a system of inspection for providers of private security

- A voluntary scheme for companies seeking SIA approval
- Companies who would like to achieve the SIA Approved Contractor status will need to comply with the SIA's set standards in order to be awarded with it
- SIA required to keep a register of approved companies (publicly viewable via the SIA's own website)
- Improves public confidence
- Promotes continuous professional development

Two main types of Law in the UK:

- **Criminal Law** (Common Law and Statute Law) - Crimes
- **Civil Law** - non-criminal law referring to civil wrongs

**Civil Law:**
This law deals with regulating relationships between two or more parties. This could be private citizens, but it can also relate to businesses and enterprises as well.

The police are not generally involved in these matters, and there will not be a criminal record involved.

Most cases are resolved by one party compensating the other.

**Standard proof is on the balance of probabilities.**
Some examples of Civil matters:

**Libel** - printing or publishing false information that is damaging to a person or business

**Slander** - similar to libel; however, the false information is spoken as opposed to printed/published material.

**Trespass** - committed by someone on someone else's property without consent, note that consent can be withdrawn and if somebody then fails to leave, they would be a trespasser.

**Employment Law** - Unfair dismissal tribunals etc

**Family Law** - divorce and child custody cases

**Contractual Law** - Contractual breaches

**Personal Injury Law** - if somebody is injured through no fault of their own

**Criminal Law:**

The purpose of Criminal law is to deter and punish.Criminal law is made up of two parts - **Statute Law** (Acts of parliament) and **Common Law** (laws based on past judicial decisions over the centuries).

Example of Statute Law - Private Security Industry Act 2001 (any law that ends with the word Act and a date would be a statute law that has been passed by parliament.

Example of Common Law - Murder, this law has existed for centuries and was not passed through parliament but instead was created over the centuries by judicial decisions.

All crimes are:

- Investigated by the police
- Handed to the Crown Prosecution Service (CPS) for prosecution through the courts
- Tried via a crown court (Indictable offences) or magistrate court (Summary offences)
- Those found guilty of crimes will be punished via the courts and receive a criminal record

**Standard of proof is beyond reasonable doubt**

**Examples of Crimes:**

- Assault
- Murder
- Rape
- Theft
- Domestic Violence
- Child Abuse
- Arson
- Kidnapping

**Useful definitions of crimes:**

**Theft**: Taking something that does not belong to you to deprive the owner of it permanently

**Robbery**: Theft using force or threat of force

**Burglary**: Entering a building or part of a building as a trespasser to commit further offences (assault, robbery, theft)

**Criminal Damage**: A person either intentionally or recklessly causes damage to someone else's property without lawful excuse

**Types of Assault**: (Listed in the least to most serious offences)

**Common Assault** - A person is guilty of common assault if they either inflict violence on another person – however slight this might be – or make that person think they are about to be attacked. Examples are slapping, poking, pushing and spitting as well as threatening behaviour. No marks need to be left on the victim. The maximum sentence is six months in prison.

**Actual Bodily Harm (ABH)** - Any injury that interferes with the health or comfort of a victim can be defined as ABH, such as bruises, scratches or bite marks. 'Actual' harm refers to the significant consequences caused by an assault, meaning physical and psychological injuries need only be of minimal detriment to health, but this must be proven. The typical injuries incurred are, broken nose, broken or lost teeth, minor fractures and minor blood loss, a brief loss of consciousness. Maximum 5 years imprisonment or a fine / community service order depending on if its a first offence.

**Grievous Bodily Harm (GBH)** - Severe accidental harm caused to a person, this is likely to end up in long term incapacity and the possibility of not making a full recovery from their injuries. Typically permanent facial scarring will also be charged as GBH, other examples are, severe blood loss, coma, long term incapacity, broken bones, long term recovery periods. The maximum sentence is up to 5 Years imprisonment.

**Grievous Bodily Harm with intent** - The injuries would be the same as the ones listed above for GBH, however in this offence the intent to cause those injuries is provable in court and therefore this is a much more serious offence with a higher sentence of up to life imprisonment.

**Attempted Murder** - Attempted murder depends on an intention to kill and an overt act towards committing homicide. Attempted murder is only the planning of murder and acts taken towards it, not the actual killing, which is the murder. This makes the offence very difficult to prove, and it is more common for a lesser charge to be preferred under the Offences against the Person Act 1861.

**Murder** - The act of murder is defined in common law in England as a person of sound mind causes the death of a human being either intending to kill that person or attempting to cause grievous bodily harm that results in death. The intention must be provable in law.

**Manslaughter** - applies where a person has caused the death of another, but they have done so without the intention to kill or cause grievous bodily harm.

**Involuntary manslaughter** - occurs when an unlawful and dangerous, or grossly negligent act or omission causes someone else's death.

**Security action in Sexual Offences**: Corroborative evidence of a recent complaint is significant in allegations of rape, as is the condition and state of mind of the complainant. If a person makes a complaint of rape to a member of the door staff, they should make a careful note of the time they made the allegation, the words they used, their demeanour, state of clothing and injuries. Report to the police as soon as possible and preserve evidence and cordon off the area where the alleged crime took place.

### The Private Security Industry Act 2001

This law was passed through Parliament in May 2001 and came into force in 2003. Its main aim was to set, maintain and raise standards in the UK's private security industry. In order to enforce and manage the new law, the government formed a new body called the **Security Industry Authority**.

Part of the SIA's main aim is to protect the public and licence people working in certain sectors within the UK's private security industry. By doing this the SIA hoped to remove criminal elements from within the private security industry.

Current licensable activities within the Private Security Industry:

- Door Supervisor
- Security Officer
- CCTV operator
- Cash and Values in Transit (CVIT)
- Close Protection
- Keyholding
- Vehicle immobilisation (only in Northern Ireland)

**The Human Rights Act:**
The European convention of human rights was drafted after WW2, the UK signed up to it in the 1950s, and it is now fully incorporated into our law. Everyone is entitled to basic human rights; we must be careful not to breach anyone's human rights in the course of our duties.

**The Rights relevant to us:**

**Article 2** - Right to life

**Article 3** - Prohibition of torture

**Article 5** - Right to freedom

**Article 6** - Right to a fair trial

**Article 7** - No punishment without law

**Article 8** - Right to privacy

**Article 14** - Prohibition of discrimination

**The Equality Act 2010 (brings the following previous acts under it)**

- Equal Pay Act
- Sex Discrimination Act
- Race Relations Act
- Sex Discrimination Act
- Employment Act
- Disability Discrimination Act

**Protected Characteristics (do not discriminate directly or indirectly based on):**

- Race
- Ethnicity
- Sex
- Sexual orientation
- Country of origin
- Age
- Colour
- Religion
- Disability
- Gender Reassignment
- Marriage/Civil Partnership
- Pregnancy
- Maternity

Areas where equal opportunities legislation applies:

- Recruitment
- Access to training
- Pay and benefits
- Promotion opportunities
- Terms and conditions

- Redundancy
- Dismissal

It is the responsibility of the employer to ensure that reasonable adjustments are made in relation to equal opportunities in the workplace

**Examples of Reasonable Adjustments in the workplace:**

- Providing disabled parking
- Reallocation of work that a disabled employee cannot do
- Providing a piece of equipment
- Swapping equipment
- Allowing regular breaks

**Key meanings:**

**Prejudice**: Prejudgement before being aware of all of the facts

**Stereotyping**: A widely held belief that is often overly simplistic of a particular type of person because of their association with a particular group

**Discrimination**: Where someone is treated less favourably than another based on a protected characteristic

**Indirect Discrimination**: Applying the same conditions to everyone but the proportion of a certain protected group who can apply is smaller

**Harassment**: Unwanted conduct relevant to a protected characteristic

**Victimisation**: Treating someone unfavourably because they have raised a complaint

**Vicarious Liability**: Refers to a situation where someone can be held liable for the acts or omissions of another person. Example: A company can be held liable for the acts and omissions of its employees

### Data Protection Act of 2018

This law was updated from the original Data Protection Act 1998 and now fully integrates the European GDPR legislation. It sets out to protect individuals' data and how it's processed and who can have access to it.

**Principles of Data Protection:**

1. Processed fairly and lawfully
2. Obtained for specified lawful purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for any longer than necessary.
6. Processed in accordance with the rights of the subject
7. Kept securely
8. Not transferred to any other country without adequate protection.

**Data Subject** - means the individual who is the subject of the data.

**Data Controller** - The person who determines what data is collected and for what purposes and how the data will be processed

**Data Processor** - Anyone (other than an employee of the data controller) who processes the data on behalf of the data controller.

**Example**: A Supermarket (**Data Controller**) employs a third-party security company to run their CCTV system. The third-party security company is the **Data Processor**. Any customer who is captured on that CCTV is the **Data Subject**.

### The use of Body worn cameras and their restrictions:

As technology improves more and more security organisations are using body worn cameras that are worn by security personnel in the course of their duties. While this technology is very helpful in protecting staff there are certain rules and restrictions that must be followed when using such devices.

### Storage of recorded images:

- This is classified as potential personal data so therefore must be stored securely in compliance with the Data Protection Act 2018
- The images and videos recorded can only be viewed by those authorised to do so

### Recording of information in Notebooks:

- This information may also fall under the Data Protection Act 2018 so needs to be kept securely and only reviewed by authorised personnel

### What does an arrest mean?

When we refer to arrest, we need to think of it in the context of a citizen's arrest. While there is no legal definition of a **citizen's arrest** essentially it is the taking or restraint of a person from their liberty so that they shall forthcoming to answer for alleged crime or offence.

A "citizen's arrest" is no longer the term applicable, the **Serious Organised Crime & Police Act 2005** abolished the statutory concept of the "arrestable offence". A constable may now arrest for any offence in appropriate circumstances.

This Act inserted section 24A into the Police & Criminal Evidence Act 1984 allowing a person other than a constable to arrest without a warrant in certain circumstances. The offence must be indictable (bilking, or refusing to pay, is indictable

The **Police & Criminal Evidence Act 1984: 24A** Arrest without warrant: other persons (1) A person other than a constable may arrest without a warrant— (a) anyone who is in the **act** of committing an indictable offence; (b) anyone whom he has reasonable grounds for suspecting to be committing an indictable offence.

**Security operatives must be very careful when carrying out an arrest, they need to be aware that if they do not follow the procedures correctly and call the police immediately, they could be breaking the law.**

Security Operatives do not have any extra powers with carrying out an arrest.

The law says that we can carry out an arrest on anyone carrying out an indictable offence (serious offence) or anyone who we have reasonable grounds for suspecting that they are committing an indictable offence.

We only carry out an arrest if there is no police present to carry out the arrest.

### Reasons to arrest a suspect:

- **Causing physical injury to themselves or another person**
- **Suffering physical injury**

- **Causing loss of or damage to property**
- **Making off before a police officer can take responsibility for them**

Only carry out an arrest if you witnessed the **indictable offence (serious offence tried in the Crown Court)** being committed or you are confident that the suspect carried out the offence. Because of the seriousness of detaining someone, you need to be reasonably sure that the person detained carried out the crime. All evidence must be passed across to the police upon their arrival.

Also, remember that after the arrest, you are fully responsible for the wellbeing of the individual detained.

**Procedure for carrying out an Arrest:**

- Introduce yourself
- Inform the person that they are under arrest
- Give them the reason for the arrest
- Inform them that the police will be called
- Call the police immediately

**When the Police arrive:**

- Hand the suspect over to the police
- You may be required to give the police a written statement
- You may be required to attend court

**Important to remember:**

- The suspect must be continually observed.
- If you need to hold them in an office/room until the police arrive, always have a witness with you and preferably with CCTV in operation.
- Always inform the person that they are under arrest and the reasons for the arrest.
- Call the police as soon as is reasonably possible after detaining the suspect.

**Typical Crimes that a Security Operative can arrest are:**

- Illegal possession of classified drugs
- Rape/Sexual Assault
- Serious Assault
- Theft
- Burglary
- Criminal Damage
- Murder
- Arson
- Weapon offences
- Robbery
- Breach of the peace

**Breach of the peace:** *any disorder or disruption to the peace in public or in private that results in violence, the threat of violence or provokes violence from another". Is called a Breach of Peace*

**The police can only arrest drunk and disorderly behaviour, Security Operatives and members of the public cannot detain a person for drunk and disorderly conduct and instead should contact the police.**

**An Arrest should always be a last resort for the following reasons:**

- Taking someones liberty is a serious matter
- Should only be done for an indictable offence
- False imprisonment could lead to allegations of kidnapping
- Could lead to civil or criminal prosecution of the security operative making the arrest
- Could increase the risk to all staff

**Actions to be taken following an arrest:**

- The arrested person is now the security operative's responsibility
- Ensure own safety
- Ensure the suspects safety
- Ensure any evidence is preserved
- Hand person over to police, explaining reason for arrest
- Inform police of any extra evidence of offence (witnesses, CCTV, property)
- Record arrest in line with local policy
- Assist police with a statement if required
- Attend court at a later date if required
- Identify how to work with the Police in relation to arrest procedures

**Use of force when carrying out an arrest:**

The Criminal Law Act 1967 allows for reasonable force to be used when detaining a suspect.

**Criminal Law Act, 1967 (Section 3, Para 1)**

Any person may use such force as is **reasonable** in the circumstances; In the prevention of crime or; In effecting or assisting in the lawful arrest of suspected offenders or persons unlawfully at large.

**Reasonable** = Necessary + Proportionate

Was it necessary to use force in the first instance and was the level of force used proportionate to the level of threat faced by all parties involved?

Reasonable force is the amount of force that can be used to protect yourself or your property from attack. It can be used to prevent crime or when detaining someone through a citizen's arrest. It can also be classed as "legal force"

**Suspect Descriptions:**

Suppose the suspect is released before the police arrive to take responsibility for them. In that case, we need to know how to describe them, giving clear descriptions of people is also crucial for report writing. Below is a list of things to remember to include when giving a suspect description; this is known as the alphabet method and is an easy way to remember what to include:

A = Age (approximately)
B = Build
C = Clothing
D = Distinguishing Marks
E = Ethnicity
F = Face
G = Gender/Gait (how they walk)
H = Height/Hair (Height should be approximated)
I = Idiosyncrasies (odd behaviours, habits)

Also, remember to include their direction of travel and last known location as well as the time they were last seen.

**Example:**

"The suspect was a white male, approximately six feet tall with a medium build. His complexion was fair and he wore a moustache. He looked young, perhaps between 20 and 25 years of age. He was wearing dirty blue jeans, a white, short-sleeve tee shirt with a logo on the back, and athletic shoes. He wore a tattered, black cap, and his hair, blonde in color, hung out the back of the cap to about shoulder length. He ran out of the store with a brown bag in his left hand. As he ran, he carried his right arm across his chest as if it were in a sling. A driver was waiting for him at the far edge of the store's parking lot in a dark blue Ford Fiesta (maybe 1990). The suspect climbed in the passenger door of the pickup and it sped off onto 4th Street."

# CHAPTER 4 Health and Safety

In the UK, all health and safety matters are usually dealt with by the Health and Safety Executive (HSE). They are empowered by the government under The Health and Safety at Work Act 1974. This legislation is set out to encourage high standards of occupational health and safety in the workplace; breaching of the act can result in fines and custodial sentences and a criminal record.

Everybody on the site (both legally and illegally) are covered under this law.

**Responsibilities of Employers to provide:**

- Safe plant, machinery and equipment
- Safe system of work
- Safe access and egress
- Written safety policies
- Training

**Responsibilities of Employees/Self-employed:**

- Follow all safety procedures.
- Attend Training
- Wear PPE
- Correct operation of all equipment
- Look after their own safety.
- Look after the safety of anyone affected by their acts and omissions.

**Hazards and Risks:**

- Hazard - anything that has the potential to cause harm
- Risk - the chance that harm could happen in certain circumstances

**Typical Hazards:**

- Locked fire doors
- Poorly stacked materials
- Improper storage of dangerous goods

- Blocked access and egress routes
- Inadequate lighting
- Spillages
- Fires/Floods or other emergencies
- Improper use of machinery
- Sharp objects (needles, knives)
- Hazardous materials/chemicals
- Diseases
- Moving Vehicles
- Poor lighting
- Obstructions
- Noise pollution

**Risk Assessments:**

- **Identify the hazards** (What has the potential to cause injury)
- **Quantify the risks** (The percentage chance of injury occurring)
- **Evaluate control requirements** (What can be done to reduce this risk)
- **Record and monitor** (Monitor and record any accidents)
- **Inform and train** (Make sure staff are adequately trained and all training is documented)

Once the risk assessment is complete action must be taken to either eliminate/adapt/reduce the risk as much as is reasonably practicable.

## HEALTH AND SAFETY SIGNAGE:

**Prohibition (Red circle with diagonal red line)** - Not allowed.

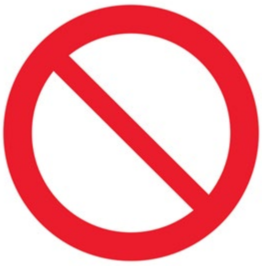
**Mandatory (Blue with white writing)**- Must comply

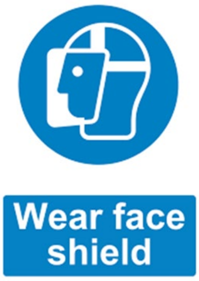
**Warning (Yellow with black writing)** - Indicates danger

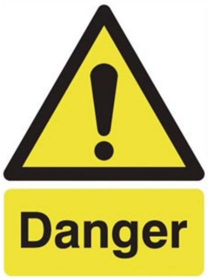
**Safe Conditions (Green with white writing)** - First aid kit/station or safe area

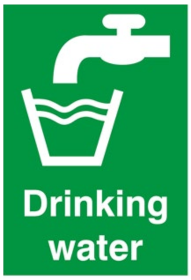
**Fire Equipment (Red sign with white writing)** - Indicates fire extinguisher etc.

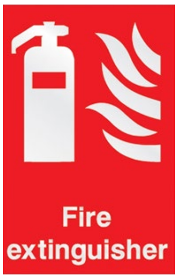
**Hazardous Chemicals (Diamond/various colours)** - Indicates dangerous chemicals.

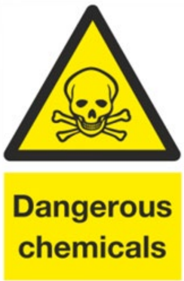










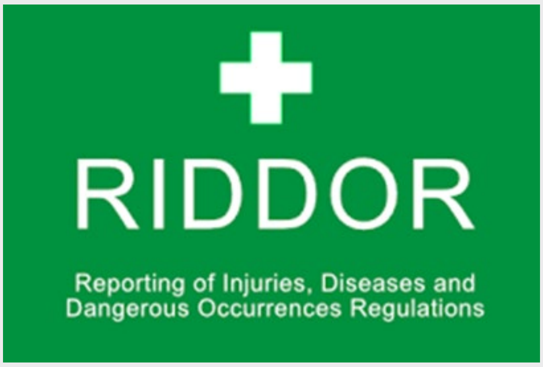


**Manual Handling:**
Before lifting consider:

- Does the object need to be moved?
- The weight of the object?
- The shape of the object?
- Ease of grip?
- Centre of gravity?
- If it’s a box, is it secure?
- Do I require any PPE?

## RIDDOR:

Certain accidents and incidents at the workplace have to be reported:


RIDDOR
Reporting of Injuries, Diseases and Dangerous Occurrences Regulations

**R**eporting of

**I**njuries

**D**iseases and

**D**angerous

**O**ccurrences

**R**egulations (2013)

## What is reportable:

- Deaths
- Specified injuries
- Injuries that result in more than seven days off work
- Over 3-day incapacitation
- Non-fatal injuries to non-workers
- Occupational diseases
- Any incident that could have caused serious injury
- Gas related incidents

## Reporting Incidents under RIDDOR:

Reports can be complete by post, telephone or online in line with organisational policies. All reports must be submitted within 15 days of the incident by a nominated responsible person

## Remember to include:

- Who (names of all those involved)
- What (What was the nature of the incident?)

- When (Time and Date)
- How (How did this incident occur?)
- Where (Location of the incident)

**Accident Books:**

Accident books should be filled in by a trained first aider as soon as is practicable after an accident in the workplace. If any first aid is required this book must be filled in.

Typical accident reports should include the following details:

- Casualty Details
- Name of the person writing the report
- Signature of the person writing the report
- When the accident happened
- How it happened
- Materials used (may need to re-order)
- Is this reportable under RIDDOR?

**Smoking:**

Smoking in the workplace was banned on the 1st of July 2007. Individual businesses can make their own decisions regarding the use of e-cigarettes on their premises as these are not currently covered under the law.

**Corporate manslaughter and Corporate Homicide Act 2007:**

As of 6th April 2008, government bodies, organisations and companies will be liable for prosecution under the Corporate manslaughter and Corporate Homicide Act 2007 and will face large fines if they are found to have caused death due to gross health and safety failings.

**Personal Protective Equipment (PPE) Examples:**

- Hard Hat/Safety shoes
- Body Worn Camera

- Gloves
- Protective clothing
- High Visibility clothing
- Stab Vests
- Torch
- Radios
- Mobile Phones

**Lone working in the Private Security Industry:**

Security operatives may work on their own on sites in certain circumstances. If this is the case the employer must do the following to make sure that the member of staff is safe.

**Steps the employer should take to protect lone workers:**

- Check calls made hourly (Phone or Radio)
- CCTV should be used to monitor the staff member
- Panic buttons could be used
- Motion detection equipment can be used

**Security operatives could be vulnerable due to:**

- Injury
- Ill health
- Violence
- Lack of Support
- Lack of communication
- Lack of rest facilities

Security operatives should always ensure that they follow all their company policies and procedures and are trained on any specialist equipment that they are required to use. They should also always be systematic and follow safe routines of work when carrying out their duties.

### Handling Personal Data/Information

When handling any personal data (either your own or someone else's) Security Operatives -

**Must:**

- Comply with all relevant legislation (DPA 2018 etc)
- Follow organisational policies and procedures
- Follow assignment instructions
- Maintain confidentiality of all information and not share it with any unauthorised persons

When handling any personal data (either your own or someone else's) Security Operatives

**Should:**

- Manage their use of social media responsibly including managing your personal settings
- Do not wear anything that is identifiable outside of the workplace (ie uniform)
- Keep person vigilance
- Do not discuss any work related issues with anyone outside of the workplace
- Do not discuss sensitive security information with anyone outside of the security or management team.
- Do not disclose any information to any unauthorised personnel

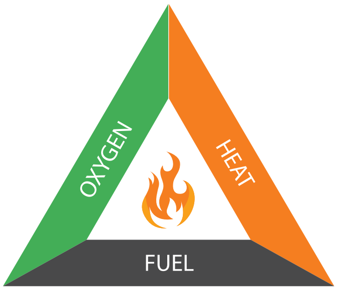
# Fire Awareness

The following should be in place in every working environment:

- A fire risk assessment
- Fire detection and warning system
- A way of fighting a small fire (Extinguisher/blanket etc.)
- Safe clearly signposted emergency exits

**Three elements that make up a fire:**

- Heat
- Oxygen
- Fuel



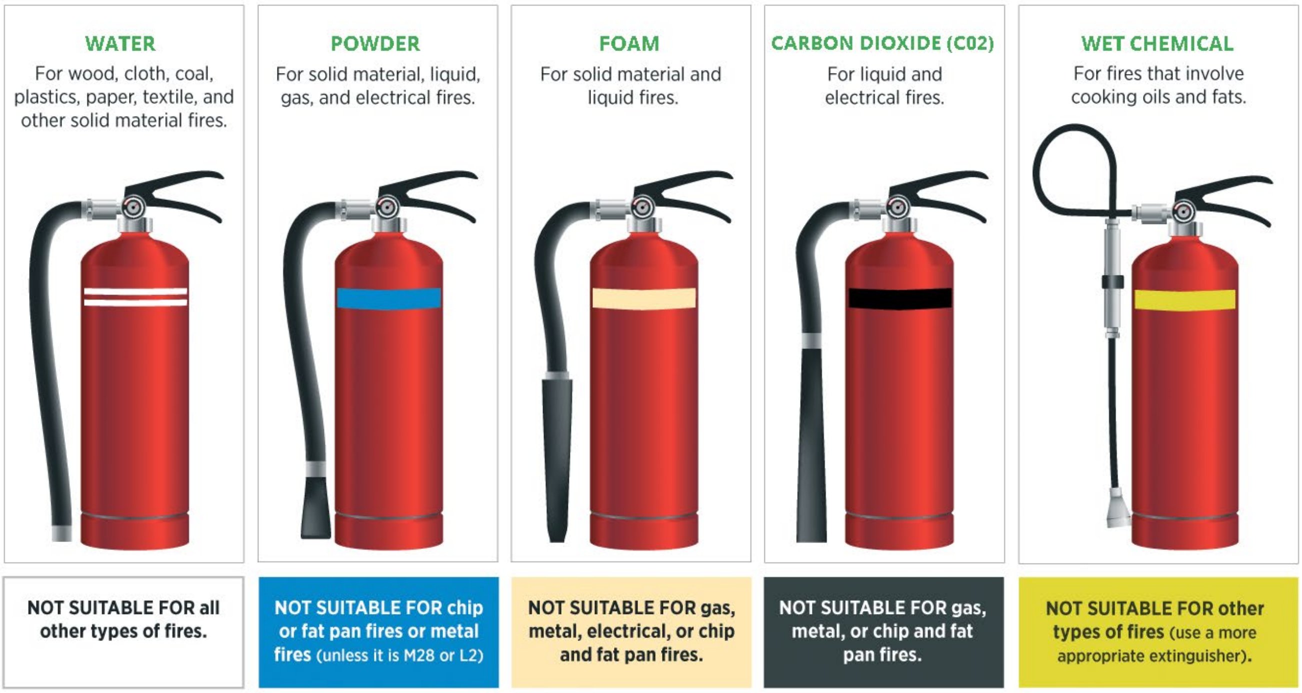
**Classification of Fires:**

| Classification: | Type: |
|---|---|
| A | Textiles (cloth, paper, solids) |
| B | Liquids (spirits, petrol etc.) |
| C | Gases |
| D | Metal |
| F | Fats and Oils |

Electrical fires do not fall into any of the above categories as electricity itself is not the fuel that is burning, unlike all of the above.

## Extinguishers:

### MAIN TYPES OF PORTABLE EXTINGUISHERS, THEIR USES AND COLOUR CODING



| WATER | POWDER | FOAM | CARBON DIOXIDE (C02) | WET CHEMICAL |
|---|---|---|---|---|
| For wood, cloth, coal, plastics, paper, textile, and other solid material fires. | For solid material, liquid, gas, and electrical fires. | For solid material and liquid fires. | For liquid and electrical fires. | For fires that involve cooking oils and fats. |
| NOT SUITABLE FOR all other types of fires. | NOT SUITABLE FOR chip or fat pan fires or metal fires (unless it is M28 or L2) | NOT SUITABLE FOR gas, metal, electrical, or chip and fat pan fires. | NOT SUITABLE FOR gas, metal, or chip and fat pan fires. | NOT SUITABLE FOR other types of fires (use a more appropriate extinguisher). |

The contents of an extinguisher is indicated by a zone of colour on the red body. Halon extinguishers are not shown since no new Halon production is permitted in the UK.

## Other Fire fighting equipment:

- Fire blankets
- Gas-based Flooding system
- Sprinklers
- Foam flooding
- Fire Doors
- Dry Risers

**On discovering a fire:**

- Sound the Alarm
- Follow organisational procedures

**Remember:**

**F**ind<br>
**I**nform<br>
**R**estrict<br>
**E**vacuate/**E**xtinguish

**Never attempt to fight a fire if:**

- You are risking your own safety
- The fire is reaching ceiling height
- Your escape route is compromised
- The area is filling with smoke
- If you have to leave the area in order to get an extinguisher

**Fire doors** - should be kept shut at all times to stop the spread of fire.

**Fire Exits** - should remain clear at all times to allow escape routes for everyone

**Fire Control Panels:**

- Helps operatives to understand the incident
- Isolate where the fire is ( panels will normally show zones with lights to indicate which sensor is picking up heat/smoke)
- They can also help in the case of a system fault/failure by isolating the which sensor is faulty

Call emergency services as soon as possible and pass all information across to them including the suspected site of the fire as well as any chemicals or gasses stored in the area

**Basic Fire Safety Controls:**

- Be observant and vigilant
- Control of fuel and ignition sources (Litter and waste disposal)
- Safe storage of any flammable materials (these should also be clearly labelled)
- Inspection and maintenance of all electrical equipment
- Avoid overloading plug points

**Portable Appliance Test (PAT)**

A full PAT test includes a visual inspection of the appliance and an in-depth check using specialised PAT testing equipment. This test checks earth continuity, lead polarity, and insulation resistance of the appliance. Doing so helps to reduce the risk of electrical fires in the workplace

**Duties of a Fire Marshal:**

- Assess fire risks
- Report hazards
- Sound the alarm in the event of an emergency
- Administer first aid where necessary
- Fight fires if safe to do so
- Ensure safe and efficient evacuation plans are in place and followed

**Fire Marshal's duty in the event of a fire:**

- Sound the alarm
- Check the area to make sure that everybody has safely evacuated
- Take roll call
- Take control of the evacuation and ensure that anyone that needs extra assistance is aided
- Proceed to the assembly point and report to the Fire officer in charge

### What is an emergency?

An emergency is any unforeseen event, sufficiently dangerous to demand immediate action.

### Types of Emergency:

- Fire
- Flood
- Power Cut
- Gas leak or explosion
- Chemical spillage
- Fight/Assault
- First Aid incident
- Bomb threat
- Suspect package
- CS gas discharge

Planning and preparation prevent poor performance.

### First Aid:

A trained first aider must be called to the scene if anyone is injured aftercare has been given a first aid book must be filled in.

### Bomb Threats/Suspect Packages:

- Raise the alarm
- Evacuate via the pre-planned bomb threat evacuation point
- Call the police

### Telephone Bomb threats:

- Call the police
- Take it seriously
- Take notes
- Use the bomb threat checklist.
- Don’t look for the device yourself.

### Example of a Bomb Threat Checklist:

Official Sensitive when Completed
Form 5474

## ACTION TO BE TAKEN ON RECEIPT OF A BOMB THREAT:

1. Remain calm and talk to the caller
2. Note the callers number if displayed on your phone
3. If the threat had been sent via email or social media see section below
4. Record the call if you can
5. Write down the exact wording of the threat:

When, Where, What, How, Who, Why, Time

## ASK THESE QUESTIONS AND RECORD ANSWERS AS ACCURATELY AS POSSIBLE:

**1. Where is the bomb right now?**
**2. When is it going to explode?**
**3. What does it look like?**
**4. What does it contain?**
**5. How will it be detonated?**
**6. Did you place the bomb, if not who did?**

**7. What is your name?**
**8. What is your address?**
**9. What is your telephone number?**
**10. Do you represent yourself or are you acting alone?**
**11. Why have you placed the bomb?**
**Record time call is completed:**

## INFORM BUILDING SECURITY/COORDINATING MANAGER:

**Name of person informed:**

## DIAL 999/112 AND INFORM POLICE:

**Time informed:**

**This part should be completed once the caller has hung up and police/ building security/ coordinating manager have been informed**

Date and time of call:

Duration of the call:

The telephone number that received the call:

**About the caller:**

Male or Female

**Threat language:** Well-spoken / Taped / Irrational / Foul / Incoherent

**Callers voice:** Calm / Crying / Clearing throat / Angry / Nasal / Slurred / Excited / Stutter / Disguised / Slow / lisp / Rapid / Deep / Familiar / Laughter / Hoarse / Other

**What Accent:**

**If the voice sounded familiar, who did it sound like?**

**Background Sounds:** Street noise / House noise / Animal noise / Crockery / Motor / Clear / Voice / Static / PA System / Booth / Music / Factory Machinery / Office Machinery / *Other

**Other please describe:**

**Remarks:**

**Additional Notes:**

**Signature:** **Print Name:** **Date:**

## ACTION TO BE TAKEN IN THE EVENT OF A BOMB THREAT SENT VIA EMAIL OR SOCIAL MEDIA

1. **DO NOT  reply to, forward or delete the message**
2. **If sent via email note the address**
3. **If sent via social media what application has been used and what was the username/ID?**
4. **Dial 999 and follow police guidance**
5. **Preserve all web log files for your organisations to help police investigation (as a guide, 7 days prior to the threat message and 48 hours after)**

**Signature:** **Print Name:** **Date:**

**END OF DOCUMENT**

**Calling emergency services:**

**Dial: 999/112**

**What to say:**

- Which service you require
- The telephone number you are calling from
- Your exact location
- Type of incident
- Number of casualties
- Extent of injuries
- Any other dangers or hazards

**Evacuation procedures:**

- Understand alarms and alarm panels
- You will stand out in high visibility clothing.
- Keep calm (your actions may cause others to panic)
- Be authoritative and professional.
- Follow your assignment instructions.
- Know your evacuation plan and assembly points for the type of emergency

**First Aid Procedures:**

- Ensure your safety
- Assess the situation
- Control the situation
- Diagnose the patient
- Save a life (treat the patient)
- Call for help (999/112)
- Know your own limits and authority to deal with personal injury
- Record the injury in the accident book

- Keep people safe
- Provide privacy whenever possible

Know your venue's policy for first aid, know who the first aiders are and where the first aid box is kept.

All first aid kits must be watertight, green with a white cross, adequately stocked and replenished if used.

**Public Reaction to emergencies:**
When emergencies occur, people could react in the following ways:

- Fight or Flight
- Freeze
- Panic

There is also a risk of crowds overreacting to situations which could lead to crowd crush incidents, Security Operatives need to be aware of this and make sure to try to exercise crowd control techniques:

- Stay Calm
- Speak in a calm clear voice and work as a team
- Command the crowd on what to do at a reasonable volume so that they can hear you

**Security Operative's Response to emergencies:**

- follow correct procedures depending on emergency
- Ensure your safety and that of others
- Report to appropriate authorities
- Act quickly, be authoritative, remain calm and encourage others to do the same
- Follow procedures for making emergency calls
- Follow escalation procedures

- Document what happened and the security teams response
- Review and evaluate the incident
- Identify how a graduated response can be applied to incidents

**Evacuation procedures:**

**Evacuation:**

This is a controlled process of emptying an area or premises of people. Evacuation can be to an adjoining area within a building or outside depending on the severity of the incident. Examples for evacuation could be flood, fire or terror threat.

**Invacuation:**

This is a controlled process of getting people into safe premises due to an incident which could cause harm to people who were outside. For example, if a person with a firearm started to shoot people in the street you would encourage everyone into the building and lock the doors for safety.

Security professionals come into contact with all kinds of customers every day while working on the front line; knowing how to communicate effectively with these customers is vital.

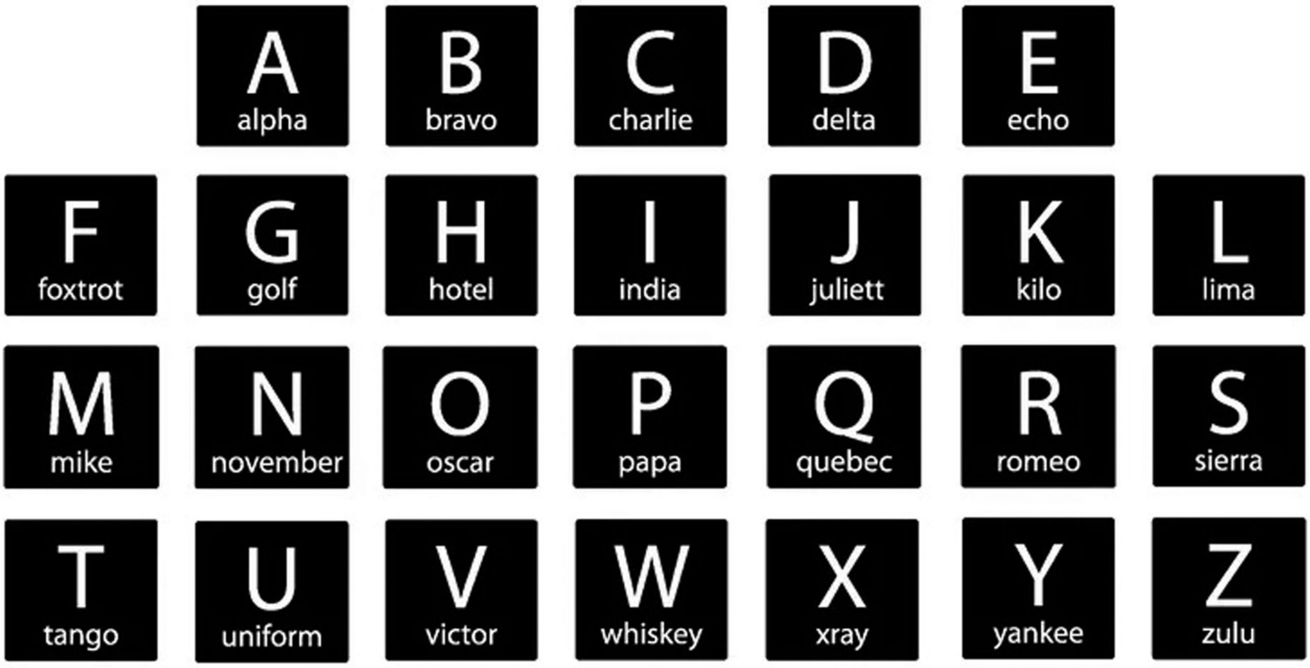
**Sender** - encodes a message

**Message** - the information itself

**Receiver** - decodes the message

**Both** parties check for understanding.

## NATO PHONETIC ALPHABET



| | |
|---|---|
| A | alpha |
| B | bravo |
| C | charlie |
| D | delta |
| E | echo |
| F | foxtrot |
| G | golf |
| H | hotel |
| I | india |
| J | juliett |
| K | kilo |
| L | lima |
| M | mike |
| N | november |
| O | oscar |
| P | papa |
| Q | quebec |
| R | romeo |
| S | sierra |
| T | tango |
| U | uniform |
| V | victor |
| W | whiskey |
| X | xray |
| Y | yankee |
| Z | zulu |

### The NATO Phonetic Alphabet:

The purpose of this method of communication enables quick identification of individuals; enables spelling of words during transmissions to avoid misunderstandings as no letter sounds the same so there is less chance of mishearing important information

### Types of communication:

- **Verbal** - made up of words and tone.
- **Nonverbal** - Body language
- **Written** - reports/statements/shift handovers

### The Importance of effective communication:

- To ensure that the message being sent is received and understood by the recipient
- Features of effective communication include choosing language and medium appropriate for message and recipient, delivering message clearly, checking understanding
- Promotes effective teamwork
- Promotes a professional establishment and service
- Prevents misinterpretation which could lead to aggressive behaviour
- Prevents misunderstanding which could lead to mistakes
- Importance of effective communication: to ensure organisational effectiveness and effective team working, to provide effective service to customers
- local policies regarding call signs allocated

### The Benefits of Working as a team:

- Promotes Safety
- Provides a professional establishment as well as safe service
- Supports colleagues
- Promotes efficiency within the security operation

**Principles of Good customer care:**

- **Beginning** - Make a good impression, show you are ready and willing to help.
- **Middle** - Find out customer needs, get any information to help, try to find a satisfactory conclusion.
- **End** - Leave the customer with a good impression of you and your organisation

**Diverse customer needs:**

Customers are individuals and may have different needs and expectations; they may come from different backgrounds and beliefs and cultures.

**Things to consider when dealing with customers:**

- Physical Difficulties
- Learning Difficulties
- Sensory impairments
- English as a second language
- Under the influence of drugs or alcohol

**Types of Customer:**

| Internal: | External: |
|---|---|
| • Your employer<br>• Colleagues<br>• Your contractual employer<br>• Your contractual employer’s employee | • Visitors<br>• Delivery personnel<br>• Emergency services<br>• Neighbours<br>• Telephone callers |

### Good Customer Service:

- Acknowledge the customer
- Be professional with every customer
- Concern yourself with customer needs
- Show respect
- Build a rapport (understanding) with your customers
- Treat people the way you want to be treated
- Serve customers to the best of your ability
- Show empathy (put yourself in their position)

### Poor Customer Service:

- Poor customer communication
- Lack of commitment
- Poor attitude towards customers
- Not paying attention to customers
- Lack of training

### Maintaining good customer care:

- Use the customer’s name if you know it.
- Say, please, and thank you.
- Make eye contact
- Explain reasons for requests or refusals
- Be approachable
- Give options and choices

### Dealing with Problems:

- Acknowledge the customer
- Establish the customers needs
- Put yourself in the customer’s position
- Accept responsibility
- Involve the customer in the solution
- See the solution through

Never criticise your colleagues or company to customers.

# CHAPTER 8 Record Keeping

**The importance of accurate record keeping:**

- To comply with the law
- To provide a clear audit trail of an incident or accident
- To prevent Security operatives having to rely purely on their memory

**Types of Records:**

- PocketBook
- Incident Report
- MG 11 (police witness statement)
- Daily occurrence book
- First Aid book
- Shift handover
- Logbooks
- Search books
- Duty sheets
- Accident reports
- Lost/found book
- Message books

All records can be used as evidence in court; they can also be used by witnesses to refresh their memories before giving evidence.

When writing a statement or report, remember to include the following:

- What
- Why
- When
- How
- Where
- Who

**Completing reports and statements:**

- Black ink
- Sign and date
- Any corrections should be neatly ruled through and initialled
- Be accurate, brief and clear
- Give a full description of people and place
- No pages should ever be removed from any report book.

**Use of Force statement remember to include:**

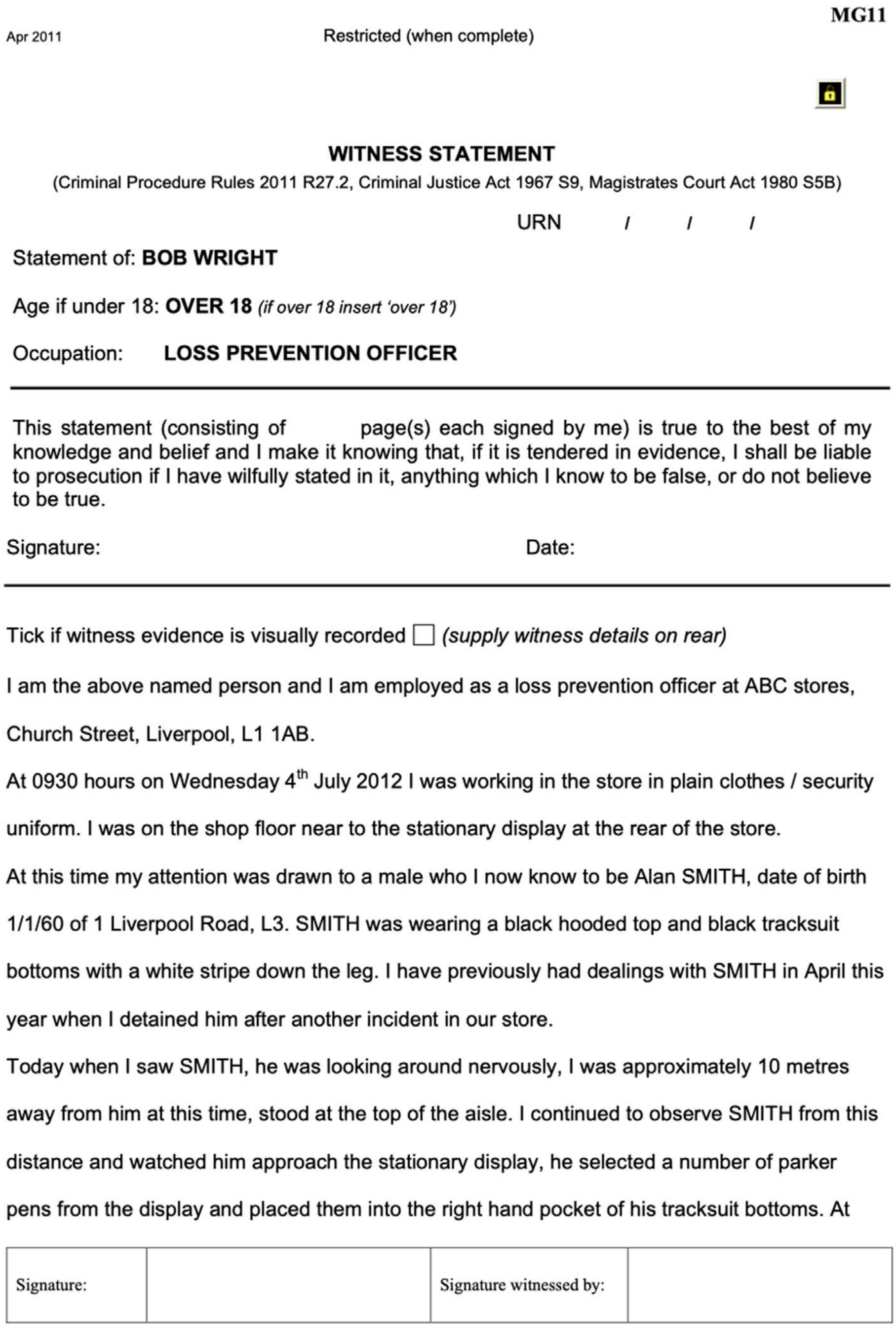
- Time and date
- Any witnesses
- What you saw and heard
- What you said and felt
- What the person said and did
- Any other impact factor
- Why force was used
- What level of force was used
- Any injuries and first aid administered
- Were the police involved?
- Was anyone admitted to hospital
- Any support to those involved and any follow up action required

**How to structure a statement:**

All statements must contain a declaration from the writer stating that the statement is accurate to the best of the knowledge and belief and must always be signed and dated.

They are written in the following format:

- Introduction (who you are and what the statement is regarding)
- Main Characters (descriptions of anybody involved)
- Set the scene (describe the area, lighting, any obstructions to your view)
- Chronological account (time order)
- Close the statement (include amount of time, any errors etc.)



Apr 2011 Restricted (when complete) **MG11**

**WITNESS STATEMENT**

(Criminal Procedure Rules 2011 R27.2, Criminal Justice Act 1967 S9, Magistrates Court Act 1980 S5B)

URN / / /

Statement of: **BOB WRIGHT**

Age if under 18: **OVER 18** *(if over 18 insert 'over 18')*

Occupation: **LOSS PREVENTION OFFICER**

This statement (consisting of page(s) each signed by me) 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 which I know to be false, or do not believe to be true.

Signature: Date:

Tick if witness evidence is visually recorded □ *(supply witness details on rear)*

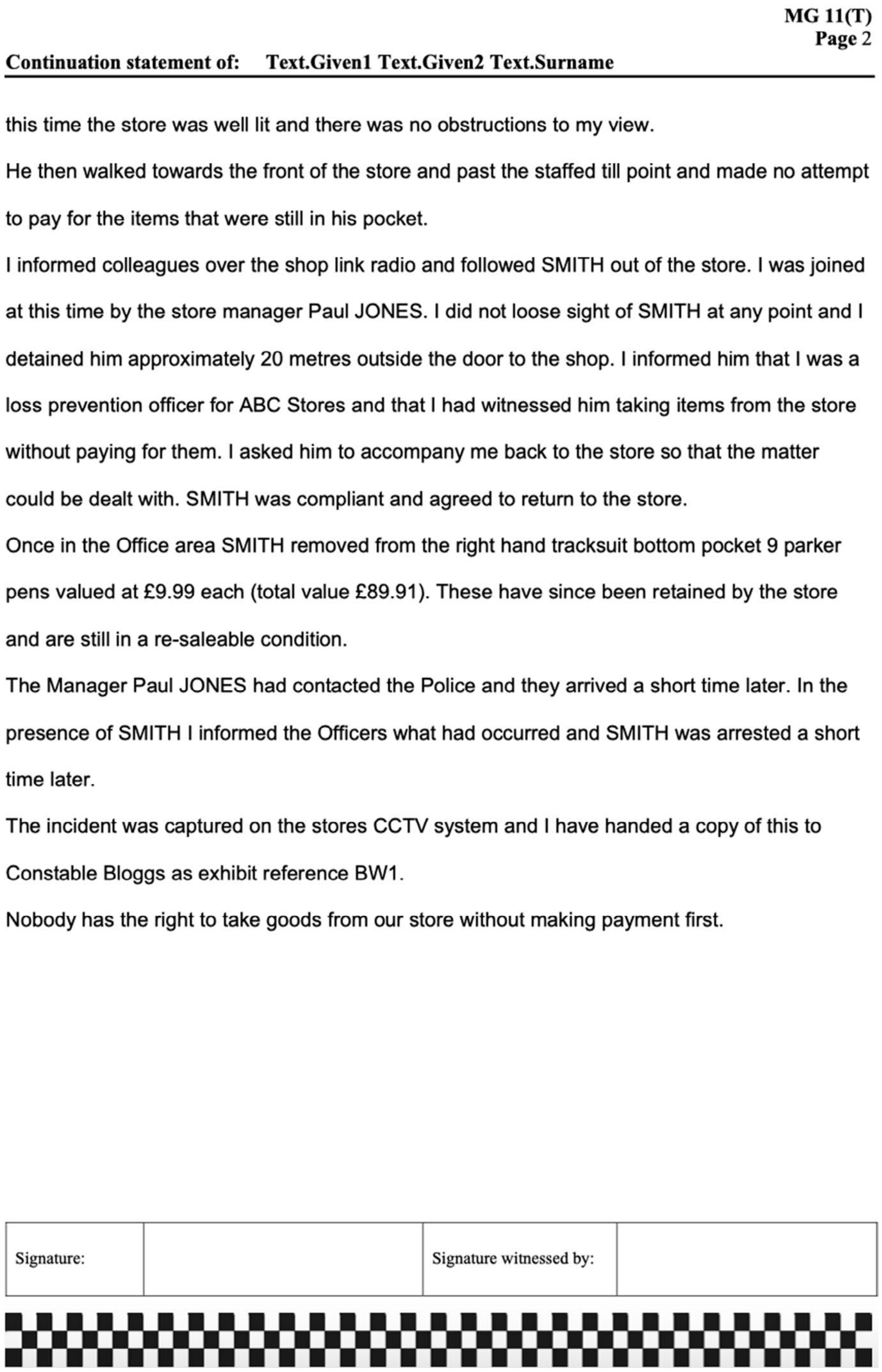
I am the above named person and I am employed as a loss prevention officer at ABC stores, Church Street, Liverpool, L1 1AB.

At 0930 hours on Wednesday 4th July 2012 I was working in the store in plain clothes / security uniform. I was on the shop floor near to the stationary display at the rear of the store.

At this time my attention was drawn to a male who I now know to be Alan SMITH, date of birth 1/1/60 of 1 Liverpool Road, L3. SMITH was wearing a black hooded top and black tracksuit bottoms with a white stripe down the leg. I have previously had dealings with SMITH in April this year when I detained him after another incident in our store.

Today when I saw SMITH, he was looking around nervously, I was approximately 10 metres away from him at this time, stood at the top of the aisle. I continued to observe SMITH from this distance and watched him approach the stationary display, he selected a number of parker pens from the display and placed them into the right hand pocket of his tracksuit bottoms. At

| | | | |
|---|---|---|---|
| Signature: | | Signature witnessed by: | |



MG 11(T)
Page 2

**Continuation statement of: Text.Given1 Text.Given2 Text.Surname**

this time the store was well lit and there was no obstructions to my view.

He then walked towards the front of the store and past the staffed till point and made no attempt to pay for the items that were still in his pocket.

I informed colleagues over the shop link radio and followed SMITH out of the store. I was joined at this time by the store manager Paul JONES. I did not loose sight of SMITH at any point and I detained him approximately 20 metres outside the door to the shop. I informed him that I was a loss prevention officer for ABC Stores and that I had witnessed him taking items from the store without paying for them. I asked him to accompany me back to the store so that the matter could be dealt with. SMITH was compliant and agreed to return to the store.

Once in the Office area SMITH removed from the right hand tracksuit bottom pocket 9 parker pens valued at £9.99 each (total value £89.91). These have since been retained by the store and are still in a re-saleable condition.

The Manager Paul JONES had contacted the Police and they arrived a short time later. In the presence of SMITH I informed the Officers what had occurred and SMITH was arrested a short time later.

The incident was captured on the stores CCTV system and I have handed a copy of this to Constable Bloggs as exhibit reference BW1.

Nobody has the right to take goods from our store without making payment first.

| | | | |
|---|---|---|---|
| Signature: | | Signature witnessed by: | |

**Statements (Section 9/MG11):**

Statements provided voluntarily in compliance with section 9 of the Criminal Justice Act 1967 (LP70s) - “s9 statements”

**Failure to complete an accurate record of events could result in:**

- Cases being thrown out of court
- No legal protection against allegations made against the security team
- Being accused of attempting to hide facts
- Loss of employment
- Loss of SIA License
- PACE (Police and Criminal Evidence Act 1984)

**Police and Criminal Evidence Act 1984:**

Although a lot of this legislation has been superseded by a newer Act (Serious Organised Crime and Policing Act 2005), PACE still relates to how evidence should be gathered, stored and processed during criminal investigations and prosecutions, this includes producing clear audit trials for any gathered evidence

**Attending court to give evidence:**

- Follow organisations Policies and Procedures
- Follow legal advice from a legal representative
- Be Punctual and prepared
- Upon arrival let the prosecutor know that you have arrived
- Dress smartly
- Don’t give the court your opinion unless asked to do so, stick to the facts
- Always address your answers to the Judge or Magistrate

**Notebooks are used:**

- For making notes while still at the scene
- Keeping details of any events
- Full report put together later
- Notebooks still official documents
- Can be used as evidence in court
- Could contain confidential information so should be kept securely
- Can be used to refresh memory before giving evidence
- Pages not to be torn out
- Erased words legible
- No blank spaces
- Corrections neatly ruled through
- Erased words legible

**Shift Handovers:**

- Areas of vulnerability
- Any issues that came up during the shift
- Any ongoing incidents
- Any hazards
- Any tasks that the next shift is required to complete
- Any messages to pass on
- Expected visitors

# CHAPTER 9 Terror threats and the role of the Security Operator

**Terrorism:**

Terrorism is the use or threat of action, both in and outside of the UK, designed to influence any international government organisation or to intimidate the public. It must also be for the purpose of advancing a political, religious, racial or ideological cause

**Terrorism Threat Levels:**

The official source of UK Threat Level is (MI5) and their website is https://www.mi5.gov.uk/threat-levels.

As well as knowing what each level means an operative would ideally need to know how it may impact the response level their location may have

**LOW** - means an attack is highly unlikely

**MODERATE** - means an attack is possible, but not likely

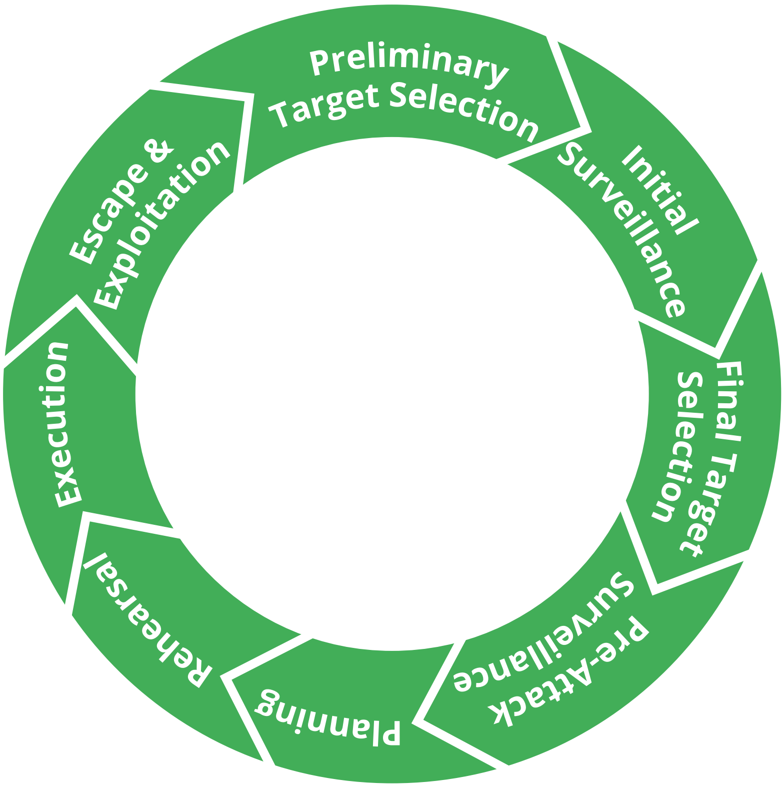
**SUBSTANTIAL** - means an attack is likely

**SEVERE** - means an attack is highly likely

**CRITICAL** - means an attack is highly likely in the near future

Security operatives need to understand how the current terrorist threat level will affect them at their own place of work, this should be outlined in their assignment instructions.

### Common Terrorist attack methods:



### Current Terrorist Attack Methodologies:

### Marauding Terror Attack (MTA)

This type of attack could use firearms, knives, sharp objects or blunt objects while on foot to attack people in the area

### Types of Explosive Devices commonly used in attacks:

- Improvised Explosive Device (**IED**)
- Person-Borne Improvised Explosive Device (**PBIED**)
- Vehicle-Borne Improvised Explosive Device (**VBIED**)
- Leave Behind Improvised Explosive Device (**LBIED**)

### Vehicle Attacks:

More often vehicles can be used as a weapon.This can be known as VAAW. Vehicles are used to target crowds and ram into people to cause severe damage such as the Westminster Bridge Terror attack which took place in London on 22 March 2017. This attack resulted in 6 deaths and 49 people injured.

### Chemical Attacks:

Chemical warfare was widely used in World War 1 which resulted in many deaths including those of civilians as there was little way to control where the chemicals travelled once they were deployed. After the war most countries agreed not to use chemical or biological weapons in future conflicts. However terrorists can manufacture weapons using many products available over the shelf and use these against the wider population

### Biological Attacks:

Bioterrorism is the use of biological agents to cause illness or death in humans, plants or animals. They can be made using viruses, funghi, toxins or bacteria. These could be naturally occurring or man made or man manipulated. They can be spread through water supplies, through the air, through food or through contaminated surfaces

### Radiological Attacks:

Commonly known as a “Dirty Bomb”, these types of devices are designed to spread radioactive material across a wide area with the intent to do harm. Radioactive materials are used in a lot of different industries including in medicine and research laboratories but can also be acquired by those who intend to do harm

### Nuclear Attacks:

Since the Atom bombs were dropped on Nagasaki and Hiroshima in 1945, no other country has used a Nuclear weapon in an act of warfare. In order to produce a nuclear weapon, a significant amount of weapons-grade plutonium needs to be acquired. It is plausible that a terrorist cell or individual could purchase a ready made nuclear weapon from a third party

### Acid Attacks:

Although not commonly used by terrorists, acid attacks can be used against individuals or groups of people. Sulphuric acid is very strong and can cause major injuries and permanent damage to victims

### Cyberterrorism:

This refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. For example hacking into computer systems, introducing viruses to vulnerable networks, website defacing, Denial-of-service **attacks**, or terroristic threats made via electronic communication

### Insider threats:

A person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes.

This includes insider knowledge of:

- Access and egress procedures
- Access to sensitive information
- Access to computer systems and networks etc
- Evacuation and assembly points

### Actions To Take in the Event of a Terrorist Attack:

Vigilant Security personnel who are confident in recognising and reporting suspicious behaviour may not only provide early warning of an attack but may even deter an attack that is still in the early planning stages.

If an attack is underway then Security Operatives must act quickly to limit the risks to all concerned, this would include early reporting and also following the government's guidelines of **RUN, HIDE, TELL**:

**Run:**

Move yourself and guide others as swiftly and as safely as possible away from the danger

**Hide:**

Once secured make sure that all members of the public as well as the team remain out of site of the attackers

**Tell:**

Call 999 or your control room as soon as possible and give as much information as is possible to the police operator, this should include things like:

- The number of attackers involved
- The last known location of the attackers
- What weapons they appear to be carrying/nature of the attack
- Known number of casualties
- Your location and situation

**Company and Venue Policies Regarding Terrorist Attacks:**

As members of front line security, it is vital that Security Operatives are well versed and understand the policies and plans in place in the event of an attack. People will look to the security team to help and lead them during these events. Knowing these procedures will be vital in both the security operative's as well as other staff members and customers overall safety.

Evacuation procedures may be different from fire evacuation procedures.

Use your local knowledge of the area to help make dynamic decisions based the information available to keep yourself, your colleagues and customers safe

**Reporting Terrorist incidents to the police:**
On contacting the police the following information should be passed across:

- What you have seen
- What has happened
- Who you saw
- What they looked like (Ethnicity, gender,  height, build, clothing, etc)
- Where the situation happened
- Where you are
- When did it happen

Be aware of the expected emergency services response times

**For non emergency activity:**
The telephone number to report suspicious activity to is the **Anti terrorism hotline:**

**0800 789 321**

This phone line is available 24/7 and is manned by specialist officers who take all reports seriously. There are also online tools that most police services offer that can be used to report activity as well.

**Public Sector Counter Terrorist Experts:**

**Centre for the protection of National Infrastructure (CPNI):** Are leaders in security, providing resources, guidance and expert advice to help protect and keep businesses secure from external threats.

**The National Counter Terrorism Security Office (NaCTSO):** is a police unit that supports the 'protect and prepare' strands of the government's counter terrorism strategy. They work directly with the Home Office.

**ACT: Action Counters Terrorism** is a government and police initiative that encourages the public to report anything that they believe to be suspicious to the police. There is a business App available as well as a free online course that all Security Personnel should all complete.

**See Check and Notify (SCaN)** is designed to help businesses and organisations maximise their safety using their existing resources, this includes training staff to look for things such as criminal activity, unlawful protest and terrorism

**The Pros and Cons of Invacuation vs Evacuation:**
**Definitions:**

**Invacuation** - Moving customers inside a building for safety reasons

**Evacuation** - Removing customers from a building

When **evacuating** personnel **out** of a building for a fire this can lead them to safety, however it can also lead to people rushing, falling and suffering from injuries as a result.

When **invacuating** personnel **into** a building that can lead them out of immediate danger, however the risk here is that people are then crowded together and could be an easy target for an attacker

**Procedures when dealing with Suspicious Items:**
Remember HOT Principles:

**Hidden** - does the item appear to be hidden

**Obviously Suspicious** - does the item have visible wires or other signs that look like it could be an explosive device

**Typical** - Is the object typical of the workplace or does it look out of place

**Remember the 4 C's:**

**Confirm** - Confirm that the package or bag doesn't belong to anyone nearby

**Clear** - Get people away from the area

**Communicate** - calmly communicate with customers and staff or police

**Control Safety Distance** - Make sure to set a cordon a safe distance away

**Distancing vs Object size:**

**Suspected device in a Rucksack or bag** - No closer than 100 m

**Suspected device in a small Vehicle** - No closer than 200 m

**Suspected device in a large Vehicle** - No closer than 400 m

In order to better visualise the distances, remember that 100 meters is roughly equivalent to the length of a football pitch

**Important:**
Do not use radios or mobile phones within 15 meters of the suspected device

**Signs of Suspicious behaviour:**
Any observed behaviour that could indicate signs of terrorism or terror related crime

This could include any of the following:

- Individuals taking an interest in the security of the site
- Making unusual requests for information
- Testing the security teams response by breaching restricted areas
- Loitering
- Tampering with utilities
- Individuals trying to avoid security staff
- Individuals carrying out activities inconsistent with the nature of the building or environment

- Forged documents or ID's
- Inappropriately dressed for the season
- Taking photographs or drawing diagrams of the site
- Parked vehicles or unattended vehicles left for long periods of time
- Multiple sightings of the same person, vehicle  or activity over a period of time

**Actions that can deter or disrupt hostile reconnaissance:**

- Ensuring visible presence of vigilent security personnel
- Frequent patrols that are done at irregular intervals
- Maintaining good search procedures
- Good access and egress procedures
- Secure emergency exits when not in use to prevent unauthorised entry

**How to respond to Suspicious behaviour:**

- Use customer service skills to disrupt potential hostile reconnaissance (example: approaching a person taking photographs of the site and asking them if they are ok or need any assistance with anything)
- Using positive and professional behaviour to act as a deterrent
- Having visible security including CCTV cameras as well as security operatives on site

**Report all suspicious activity:**

- Follow your internal procedures
- Contact the counter terrorism hotline (0800 789 321)
- British Transport Police (BTP) 0800 40 50 40 or text 61016
- Non Emergency 101
- Active Counters Terrorism (ACT) report form

**In an emergency always dial 999**

# CHAPTER 10 Keeping Vulnerable People Safe

**Recognising the duty of care regarding vulnerable People:**

- Duty of care is the moral or legal obligation to ensure the well-being or safety of others
- People may not always appear to be vulnerable so it is best practice to have the same duty of care for everyone

**Factors that could make people Vulnerable:**

Drugs and alcohol can make people vulnerable as it could lead to:

- Reduced inhibitions
- Decreased ability to make considered decisions
- Changes perceptions of skills and limitations
- Becoming overly expressive
- Aggression
- Loss of balance and spatial awareness

It can also lead to customers becoming separated from friends and possibly losing their possessions (phones, bags, etc.).

Ejecting a drunk customer could lead to unwanted attention from other customers.

While anyone can be vulnerable, this is especially true when dealing with people under the age of 18.

Other people who could be vulnerable:

- People suffering from mental illnesses
- Elderly people
- Very ill people
- People with learning disabilities
- People with physical disabilities

Not all disabilities are visible, people may be suffering with physical, neurological or mental illnesses that are invisible to an onlooker

### Sexual Predators:

A Sexual predator commits sexual crimes. A person can be a predator if they are ignorant of the fact that a drunk person cannot consent to sex.

**They may choose victims based on any single or combination of the following:**

- Gender
- Vulnerability
- Availability
- Location
- Race
- Appearance

They may also use deliberate tactics to select and engage victims (grooming).

### Identifying the behaviours of a sexual predator:

- Closely watching vulnerable people
- Buying drinks or gifts for vulnerable people
- Suspicious behaviour around certain times and venues
- Inappropriate use of technology eg phones

### Actions for Security staff:

- If you see someone being pestered, you should intervene, assess the situation and determine if the person should simply be removed from the premises or if more severe action is taken.
- Call the police if necessary.
- If you find drugs that you believe could be used to facilitate a crime, call the police.
- Suppose you see a person who appears to be heavily intoxicated, leaving the venue with someone who does not. In that case, you should intervene and try to seek some clarification on the relationship between them.

**Indicators of Abuse:**

- Restricting freedom of an individual
- Unexplained bruising
- Lack of confidence and insecurity
- Changes in appearance or cleanliness

**How to deal with allegations of Sexual Assault:**

- Follow your organisations policies and procedures
- Notify the police immediately
- Safeguard the victim
- Keep the alleged assailant away from the victim (cross contamination of evidence)
- Take careful note of the victims appearance, demeanor, state of clothing and any obvious injuries as well as exactly what they say
- Take note of the time of the complaint and when the victim says it occured

**Understanding the risks to a member of the public refused entry or ejected:**

They can become separated from their friends and find themselves alone and vulnerable. Security staff should determine what they can do in the event of this occurring:

- Is the person over 18?
- Are they under the influence of drugs and alcohol?
- Are they alone?
- Do they have their belongings?
- Do they need medical attention?

**Security Operatives should consider the following actions when dealing with vulnerable people:**

- Seeking help from street pastors/street marshals and other schemes active in the area.
- Calling a relative or friend in the case of a younger individual
- Calling a licensed taxi
- Using safe havens
- Be aware of any safety initiatives that are running such as “ask for Angela”
- Calling the police

**Ask for Angela:**

This is an initiative which can be used by anyone who is feeling vulnerable or threatened. It was set up to help reduce the number of sexual assaults carried out on nights out, customers will be made aware of it on posters in the venues toilets which encourages anyone feeling vulnerable to ask any member of staff for Angela which will inform them of their position so the member of staff can help them

**Identifying potential indicators of child sexual exploitation:**

- Children and young people in the company of older people or antisocial groups
- Young people acting in an inappropriate or sexual manner
- Children or young people intoxicated

**Visible signs that children are being trafficked:**

- Arriving and departing a location with different adults on the same day or over a while
- Children getting in or out or different cars.
- Groups of young people using bed and breakfasts with older men

**Look out for behavioural changes in children:**

- Chaotic, aggressive or sexual behaviour
- Self-harm or suicide attempts
- Showing fear in a particular company
- Having cuts or bruises
- Having unaffordable new items like clothes or phones
- Developing expensive new habits like alcohol or drug use

If you suspect child sexual exploitation is taking place, please call:

**The Police - 999/112**
**Crime Stoppers - 0800 555 111**

**Dealing with Antisocial behaviour:**

- Follow all local policies and procedures
- Speak to the person or people
- Explain the situation to them and the risks of antisocial behaviour
- Explain what will happen if they continue to behave in this manner
- Remain calm
- Make sure to your colleagues are aware of the situation and have back up if required
- Remain vigilant
- Carry out regular checks and high profile patrols
- Early intervention
- Positive non aggressive communication
- Prompt reporting of incidents
- Accurate recording of incidents
- Liaising with police and other agencies

# CHAPTER 11 Post incident Management

**Post Incident help could be available from the following sources:**

- Colleagues, management and counsellors
- Internet
- Publications
- Help Lines
- Trade Unions
- Citizens Advice Bureau

**Why accessing help following an incident is important:**

- Reduces long term problems such as depression, anxiety, fear and PTSD
- Helps to reflect on your actions and see if there is anything that can be done better in the future

**The Benefits of Reflecting on an incident:**

- Areas for improvement can be identified
- Prevents recurrence of the same problem or similar problems in the future
- Organisations can use this information for license hearings
- Recognising Trends
- Recognising poor practice
- Recognising good practice
- Making sure good practice is shared within the organisation
- Making improvements to procedures for future occurrences
- Identifying common responses to situations

**The benefits of Security Operatives contributing to improving Practices:**

- Promotes a professional service
- Increases staff safety
- Promotes Teamwork
- Increases safety for customers
- Identifies procedures and methods to deal with situations effectively

# PRINCIPLES OF WORKING AS A CCTV OPERATOR IN THE **PRIVATE SECURITY INDUSTRY**

**The Purpose of Surveillance:**

CCTV Surveillance can be used in the following ways:

- Assisting in the prevention, detection and reduction of crime, disorder or anti-social behaviour
- Assisting in the promotion of public safety
- Monitoring Traffic flow and assisting in traffic management
- Assisting in civil emergencies and counter terrorism

**Control Rooms:**

- Vary in size and function
- May be very small with one member of staff
- May be very large with many banks of monitors and many staff
- May be linked to the police

**The Roles include the following:**

**The system Owner:**

- A company, council, local authority or a person
- Pays for the equipment and cameras
- Decides where to place the cameras and what they should cover
- They are also responsible for deciding what the system is for and what is designed to achieve
- Many councils in the UK have town centre CCTV systems in operation that usually are shared with the police
- Many private control rooms
- Whenever a local authority wants to install CCTV in an area they will need to make a legal case for it
- The owner is also responsible for the operation of the system
- Signs a code of practice

**System Manager:**

- Manage the system
- Deal with staff training
- Make sure that the system is maintained
- Comply with the legal requirements
- Direct dealing with the public and handle any complaints

**Team Leader:**

- More experienced operators
- Set shift patterns
- Ensuring staffing is covered
- Day to day running of the team
- Bridge the gap between an operator and and the system manager

**CCTV Operator:**

- The person or people who operate the system
- Must have understanding of all control room equipment
- Be good at multitasking and administrative tasks
- Know how to write a report that can be used as evidence in court
- Have knowledge of the law regarding the use of surveillance
- How to maintain professional conduct at all times
- Observe all health and safety rules
- Be a good communicator both with colleagues as well as external partners (police, emergency services)
- May need to attend court

**Technical Support:**

- These are normally engineers trained and qualified to install and service the equipment
- They will have knowledge of data protection

- They will have a good understanding of how to place the cameras in positions that cover areas required and do not invade individuals privacy
- They should also have knowledge of the principle that collecting of images must be relevant, adequate and not excessive

**The data controller:**

- The data controller has a legal responsibility for any data processed through the CCTV system

**Other Stakeholders (Partners):**

CCTV Operators will often work with other partners and stakeholders in the course of their duties.

- Police
- Fire
- Ambulance
- Borders Agency
- Customs Officers
- Trading Standards
- HSE Investigations

Requests for assistance from any stakeholders could come at any time, sometimes authority would need be given, however CCTV operators should not delay in assisting these partners, even if the relevant paperwork is yet to be received as this can be delivered after the operation is over, more on this later

**Working with Stakeholders:**

- Always be willing to assist
- Communicate clearly
- Pass and receive information to and from the different agencies

## Dealing with Multiple Agencies or Multiple Incidents Effectively:

### Types of Assistance:

- Providing intelligence and Information
- Tracking, searching and securing areas
- Crowd control/Evacuation control
- Recording Evidence

### Using:

- Radio, phones and personnel
- Dedicated phone line, or radio links
- Dedicated person in the control room from an outside agency

**Confidentiality:**

- Collecting of any personal data including images that are identifiable are protected under the Data Protection Act 2018
- Any information that comes into a CCTV operator's possession falls into this category.
- Any disclosure of any information must be authorised
- Responsibility to disclose or not is placed on the person being requested for information
- If the operator is unsure they should seek clarity from their supervisor/team leader
- No unauthorised recording should take place within the control room
- No unauthorised copying of footage is permitted
- This includes any information gathered using either Body Worn Cameras or UAV's (Drones)

**Unlawful disclosure:**

- Could lead to prosecution under GDPR and Data Protection Act 2018
- Lose of SIA Licence
- Loss of employment
- Fines or imprisonment

**Freedom of Information Act (FOI):**

- This act applies to public authorities (Local Councils, or Public Bodies only)
- Requests can be made to ask for things like statistical information IE number of deaths in a hospital
- The request can refer to any information held by the authority at the time of the request being made
- Requests will be dealt with by the Data controller for the authority in question
- Requests are normally made in writing with a return address included in the request
- Requests do not have to be made in English
- Requests can be made from anywhere in the world
- All requests have to be replied to within certain timeframes

**The following may not be requested under a FOI request:**

- Subject of an ongoing criminal investigation
- Interest of national security
- Information being considered by a court
- Legal privilege
- Commercial interest/Trade secrets

**Subject Access Request (SAR):**

- Made only by or on behalf of the person who the data relates to
- Has to be responded to within a certain period of time
- Can be refused if an exemption exists
- Two Pieces of information are normally answered
    a. Is there any personal information on the subject held?
    b. What is the information?
- In certain circumstances only some of the information may be released

**The Surveillance Camera Commissioners code of practice:**

- Applies only to mainly local authorities and police forces currently
- Designed to reassure the general public that the CCTV systems are there to protect them and not spy on them
- Does not apply to private CCTV systems currently
- Established under the Protection of Freedoms Act 2012

**The 12 Principles of the Camera Commissioners code of practice:**

1. Use of surveillance cameras must be for a specific purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need
2. The use of surveillance must take into account its effect on individuals and their privacy and must be reviewed regularly
3. The use of the system must be as transparent as possible and there must be a published contact person to access information or make complaints
4. There must be clear responsibility and accountability for all users of the system
5. Clear procedures need to be produced and all who have access to the system must be fully aware of these
6. No more information should be stored than is necessary for the states requirement of the system
7. Access to retained stored images and data must be restricted to only those authorised to view it
8. Operators need to always work to their approved codes of practice relevant to the system that they are using
9. Any system images should be safeguarded against unauthorised access
10. Effective review and audit systems should be in place
11. Systems should be used in the most effective way to support public safety and law enforcement
12. Any information stored for matching purposes should be accurate and kept up to date

**The Human Rights Act 1998:**

- Applies to public authorities only
- Private individuals are not bound by this act (unless acting on behalf of a public authority
- Based on The European convention of human rights
- Became part of the UK's legislation in 1998
- Made up of 14 Articles of which some impact on the operation of CCTV
- The articles are described as **Absolute**, **Limited** and **Qualified**

**Absolute** - Cannot be restricted or limited by the state under any circumstances

**Limited** - May be limited under finite and specific circumstances

**Qualified** - Require a balance of the rights of the individual versus the rights of the community

**Articles relevant to the CCTV operation:**

**Article 3 Prohibition of Torture (Absolute right)** - Not using cameras in a degrading way

**Article 5 Right to Liberty (Limited right)** - A person has the right to move around freely unless they are arrested and sent to prison, CCTV can be used to convict, but it can also be used to prove somebody is innocent

**Article 6 Right to a fair Trial (Absolute)** - Everyone has the right to a fair trial, CCTV can be used, but it must have been obtained lawfully

**Article 8 Right to Private and Family Life (Qualified)** - CCTV cannot be used to intrude on someone's private or family life without lawful authority, because this is a qualified right there will be times where this can be lawfully done

**Article 14 Prohibition of Discrimination** - Nobody should be discriminated against for their protected characteristics (race, ethnicity, sex etc)

**Regulation of Investigatory Powers Act 2000 (RIPA):**
Sets out the lawful way in which surveillance can be carried out, in cases where Article 8 of the Human Rights Act is breached, then authority must be obtained.

It relates to 2 types of Covert Surveillance.

**Remember:**
**Covert** - Hidden cameras, people unaware of their operation
**Overt** - Visible cameras, people are aware of their operation

**Intrusive surveillance** - when viewing takes place at a residential premises or private vehicle and the camera or operator is present in that residence or vehicle or surveillance is carried out using a device

**Directed Surveillance** - carried out as part of an investigation and is likely to result in the gathering of private data about that person, it is usually pre-planned however can result from an urgent response to an event

**Local Authority Surveillance:**

- Must be approved by a magistrate
- Can be applied by local authorities to detect or prevent crime
- Can be related to the underage sale of alcohol and tobacco

**Police Surveillance:**

- Interest of national security
- For the purpose of crime prevention or detecting crime
- Preventing disorder
- Interest of public safety
- Protection of public health
- Interest of protecting economic well-being of the state
- Purpose of collecting levies or payments to any government department

**Directed Surveillance:**

- Must be for a lawful legitimate reason
- When authorised it is time limited, although it can be renewed
- All relevant paperwork must be completed and approved by the appropriate person

**If Police are authorising:**

- Police rank Superintendent or Above for pre-planned events
- Urgent cases a Police Inspector or above can verbally authorise however this must be confirmed in writing as soon as possible, the maximum time authorised is 72 hours

**Surveillance Requests:**

- If police request the operator should confirm if the request falls within RIPA legislation or not
- If authorisation is required and not received correctly the images obtained may not be able to be used in court

**Sexual Offences Act 2003:**

**Voyeurism:**

- The observation of someone (without their knowledge) doing a **private act** for the purpose of sexual gratification
- Can be carried out without the use of CCTV, however the use of recording equipment is mentioned in the act, this includes setting up and recording as well as viewing the images
- If convicted the offender can face custodial sentencing as well as being added to the sexual offenders register
- Loss of CCTV License

**Images of a sexual may be viewed and recorded if:**

- A crime is taking place
- The activity is taking place in a public space (criminal offence)
- The images can be used in a prosecution for an offence
- The is a potential of an assault taking place
- One party appears to be heavily intoxicated and may not have given consent
- Signs of a struggle

**What is a Private Act?**

- A person is naked, or in underwear
- A person is using a toilet
- A person is doing a sexual act that would not be carried out in public

**The Sex Offenders Register:**

- Details of any person who has been cautioned, convicted or released from prison since 1997 for a sexual offence against an adult or a child
- CCTV operators may be requested to monitor sex offenders
- This could be a formalised request (normally from the police)
- It may be that this is a known offender
- Operators need to ask themselves if the monitoring is reasonable and proportionate
- Confidentiality is essential
- Images must be viewed only by those authorised to view them
- It may be that RIPA needs to be considered

**Sexual Predators:**

- They commit sexual crimes
- Can be male or female, any race, level of intelligence or profession
- Usually confident, sober, friendly and helpful

**Victims can be picked based on:**

- Gender
- Age
- Race
- Availability
- Vulnerability
- Location
- Time of day
- Appearance

**Child sexual exploitation Warning Signs:**

- Young children/young people who are intoxicated who are with older people who are not intoxicated
- Children in the company of older antisocial groups
- Children acting in inappropriate or sexual way

**Signs to look out for in children who may be being exploited:**

- Developing expensive new habits
- Changes in behaviour
- Having injuries
- Time away from family or home
- Showing fear in certain company
- Sexual behaviour
- Self harming or suicide attempts

**Signs of Child Trafficking:**

- Children checking into hotels or Bed and Breakfasts with older people
- Children getting into and out of a number of different vehicles in a short space of time

- Arriving and departing with different adults over a short space of time
- Call crime stoppers on 0800 555 111 or 999 in an emergency

**Information Commissioner's Office Code of Practice**

- Issued under the Data Protection Act 2018
- Reassures public that the system is being used fairly and lawfully
- Its run with integrity
- How data is collected and stored
- Allows for the public to request access to any personal images (Subject Access Request)stored on the system

**It covers the use of:**

- ANPR Systems
- Body worn cameras
- Unmanned Aerial Vehicles (UAV)
- Any system that captures any identifiable images

**Assignment Instructions (AI's):**

These are CCTV operators' set of guidelines as to what they need to do on any particular site that they are working on, they can differ from site to site and will be designed by both the security company and the company that they are providing security for.

They help make sure that CCTV Operators are:

- Following the law
- Maintaining company policies
- Complying with client instructions

**SIA Standards of Behaviour:**

- Professional Appearance
- Professional Attitude and Skills
- General Conduct
- Organisation/Company Standards and Values

**Unmanned Aerial Vehicles:**

- The airspace in the UK is controlled by the Civil Aviation Authority (CAA)
- The Air Navigation Order 2016 (ANO) was established to set the latest rules for aircraft operating in the airspace of the UK
- UAVs are restricted from operation within airport airspace
- If a CCTV operator is working and sees an unauthorised UAV in the area they should immediately report it to the police

**Operational Procedures:**

- Also known as Assignment Instructions (AI’s)
- Explain the day to day running of the system
- Not made public
- Each system will have its own AI’s that should be followed

**Compliance:**

Compliance with AI’s ensures:

- Evidence is more likely to be admissible in court
- Public is reassured
- Operators are in compliance with the Data Protection Act and any other statutory obligations
- Public trust in the system
- Standards are met and can be raised
- Partners have clear understanding of working relationships
- Operators who are compliant with their AI’s will be protected from allegations of misuse

**Operational Procedures Manual can include the following information:**

- Access to the Control Room
- Emergency Procedures
- Health and Safety
- Proactive use of CCTV
- Duties and shift patterns
- Image/Media Management
- Communication and Radio Procedures
- Legal Guidance
- Key handling
- Fault Reporting Procedures

- System Failure Actions
- Maintenance
- Essential/Useful Telephone numbers
- Releasing of Recorded information

**The System Must Be:**

- Operated, controlled and maintained to a set procedure
- This allows for standardisation and consistency for all control room staff
- Establishes the boundaries of of the procedures

**Operator Statements:**

- Whenever any footage is taken from the control room as evidence, it is highly likely that the operator on duty at the time of the incident will be required to also submit a statement
- This statement will need to have something to the effect that it is true to the best of their knowledge and belief and that if they have willfully withheld evidence they are liable to prosecution
- A good statement may not be challenged in court, that could save the operator from having to appear in court

**Magistrate Court:**

- Lower criminal court with all cases heard by either 2 or 3 Magistrates or a District Judge
- No Jury in a Magistrates court
- Holds Trials for summary offences
- Can also hold preliminary hearings for more serious offences
- Clerk of the court acts as a legal advisor to the magistrates

**Crown Court:**

- Indictable offences go to the crown court
- Cases heard in front of a preselected jury from the general public
- A judge normally presides over cases

**Attending Court:**

- Always arrive in good time and let the Crown Prosecution Service know that you have arrived
- Read through your statement to remind yourself of the event in question
- You are likely to be asked several questions from both the prosecutor and and the defence
- Always address your answers to the judge or jury (magistrate if its a summary case)
- Keep your answers accurate, brief and clear
- Do not give your opinion unless asked to do so
- If you do not know the answer to a question then say so

**Evidence:**

Information presented to a court that can be used to prove someone's guilt or innocence

Evidence can be used to prove or disprove the following facts:

- The identification of the accused
- If they did or did not commit the offence for which they were accused
- Any provable intent or knowledge

Evidence must be **relevant** and **admissible** to court

**Types of evidence:**

**Primary** - Original items used in a Crime,ie original CCTV recordings
**Secondary** - Copies of primary evidence, ie copies of CCTV footage
**Direct** - Something you see hear or experience yourself
**Circumstantial** - Facts that tends to point to a conclusion
**Opinions** - Expert opinion, forensic specialists, doctors etc
**Hearsay** - Generally unreliable, second-hand information (is admissible in certain circumstances (police statements in domestic violence cases where the victim refuses to cooperate)

**Oral** - First hand evidence given verbally by a witness

**Documentary Evidence** - Any written, drawn or printed document, as well as CCTV images or any media that can preserve information

**Forensic Evidence** - Fingerprints, DNA, Blood, Firearm, ballistics etc

**Real Evidence** - Anything that is produced as an exhibit to the court

**Corroboration** - Evidence that supports other evidence

**Exhibits** - Items that are connected to a case, ie DVD's, weapons etc

### Perjury:

Making a statement under oath that you know to be false or do not believe to be true is a criminal offence.

### CCTV Evidence:

As well as the images being submitted in evidence, CCTV operators will also be required to submit a statement of the events as well.

### Proof:

- Criminal Courts need to prove evidence shows beyond a reasonable doubt that the defendant is guilty
- A defence team will try to create doubt in the eyes of the court in order to get their client acquitted
- In civil matters proof depends on a balance of probabilities ie the court looks into what is likely to have happened
- In civil matters it is up to the claimant to prove their case not the defence

### Tribunals:

- Sit as a panel
- Have a legally qualified Chairman
- Certain members have expertise
- Hear evidence
- Decide the case
- Have some limited powers to impose fines and penalties, compensation and costs

**Police and Criminal Evidence Act 1984:**

- Ensures evidence is treated correctly so it can be used in aid of prosecutions
- Lack of audit trails, missing information etc  on evidence may lead to it being inadmissible in court

**Producing evidence:**

- Incident recorded
- Logs complete
- Police attend, view footage and then formally request footage as evidence

**Two Copies of Evidence produced:**

**Master Copy** - Placed into an evidence bag and sealed with the bag number logged, stored securely until time of the trial

**Working Copy** - Handed over to police or agency for viewing and disclosure, signed out by officer

- Full written statement complete by operator
- All actions logged, always preferable to have the same operator complete all actions for evidence continuity (preferably the same operator who was recording the incident itself, although this is not always possible)

### CCTV Systems:

Cameras are connected by a method of transmission to a monitor and a type of recording device such as a hard drive (modern system) or Video cassette (older system).

### Systems likely to include:

- **Cameras** - (covert, overt, semi covert) fixed or pan tilt zoom (PTZ)
- **Lens** - digital zoom, fixed, zoom
- **Transmission methods** - cable, airwave, radio, microwave, fibre optic IP
- **Control systems** - Joystick, mouse and keyboard etc
- **Monitors** - single monitor or banks of screens
- **Recording system** - hard drive
- **Multiplexer** - Allows more than one camera to display on a monitor
- **Method of transferring recording** (USB's, disks etc)

### Types of Cameras:

- **Overt** - These cameras are clearly visible and people can see in general which direction they are aiming
- **Semi-Covert** - Camera is visible however it normally housed in a dome and therefore it is difficult to see what direction it is pointing
- **Covert** - Cameras are actively hidden from view, they could just be out of sight or disguised
- **PTZ** - These cameras can be panned (left or right movement), tilted (up or down movement) or zoomed (image magnified)
- **Fixed** - Camera is prefixed into a position and cannot be moved other than manually going out to the camera and physically move it
- **Day/Night** - Modern cameras can switch to night view which will normally in black and white
- **HD/UHD** - Higher resolution cameras allow for clearer images that can be digitally zoomed in to a greater level without the image becoming pixelated

- **Analogue** - Limited picture quality as they are sent as TV signals
- **Digital** - HD and UHD quality images possible
- **Infrared** - High frequency used at night

### Camera lenses

- Used to focus light onto a light sensitive silicon chip
- Keeps the image focused
- Can be automatically focussed or manually operated
- Allows operators to zoom in and refocus the light
- Digital zoom is achieved through zooming in of a digital image and does not involve the lens itself so it can become limited by image quality (the higher the resolution of the image, the better the digital zoom capability will be)

### Image Sensors:

- This is a small panel that the lens directs light to be converted into digital information
- CCD - Charged Coupled Device
- CMOS - Complementary Metal Oxide Semiconductor

### Power:

- All cameras require electrical power to operate
- Usually low voltage on modern cameras

### Transmission:

- Cable
- Radio
- Fibre optic

### Digital Recording:

- Digital recording is now the preferred method of recording images on CCTV
- Cassette recorders have now been replaced with Digital Video recorders (DVR) and Network Video recorders (NVR) this makes storage as well as reviewing images has become a lot easier for controllers, also the data is better preserved digitally
- Physical storage space requirements now much smaller

### Algorithms (Machine learning and AI)

- Smart systems now exist that can track odd or out of place behaviour and alert the operators.
- This can be done simultaneously across multiple systems, something that a person would not be able to accomplish on their own.
- Facial recognition and tracking systems are also in use in many sectors as well.

### ANPR (Automatic number plate recognition):

- ANPR systems automatically scan and search databases for any information for a specific vehicle, this could be used by police but is also used in many car parks to record vehicles entering and exiting
- Cameras need to be set up in a way where they have a clear unobstructed view of the registration plate as vehicles pass by

### Facial recognition:

- Software can also be used to digitally recognise faces
- These types of systems are becoming increasingly used a border control posts at airports where passengers scan their passports and then look up into a camera to be checked into a country

### Biometric Systems:

- Iris or fingerprint scanners are also now in common use, both as access control and recognition systems.
- Software can also be used to record clothing for later identification on police systems.

### Other types of recognition systems:

- Gait recognition - systems that recognise how a person walks
- Behavioural recognition - systems recognising different patterns of behaviour and notifying the operator of any changes to that pattern

### Motion Detection:

- System only records changes in the image, this way an area with little or no movement is only recorded when there is movement
- This type of system can save a lot of storage space as it records much less often

### Public Address Systems (PA):

- Some systems also have speakers attached near to the camera systems so the operator can warn people that they are being watched
- Normally used by councils in town centres

### Mobile CCTV Vehicles:

- Vehicles set up with CCTV systems
- Can be brought to a trouble hotspot, ie Town Centres at night
- Can be deployed at short notice

### Thermal Imaging cameras:

- Sense heat can display heat as a different colour to the colder surrounding area
- Usually used by police helicopters or military FLIR pods (Forward looking infrared)

### Unmanned Aerial Vehicles (UAVs/Drones):

- Have been used for military purposes for quite some time
- Are available commercially for filming to replace helicopters (far more costly) for aerial shots
- Also used in wildlife tracking (again as a cheaper option)
- Are also widely available for entertainment

- Normally will have cameras and recording equipment on board
- Drone use is restricted, if a CCTV operator spots any unauthorised use they should report it to the police

**Functional Checks:**

- Ensure that all equipment is functioning properly
- Minimises system failures

**Systems to check:**

- Cameras
- Controllers
- Monitors
- Recording Equipment

Any faults should be reported as per company procedures

**CCTV System failures:**

If a system fails the operator must:

- Let their shift manager/team leader know immediately
- Follow any rebooting/restarting processes
- Contact an engineer
- Fill out any reports required
- If a failure happens out of hours also remember to include details of the failure on the shift handover

**Surveillance Techniques include:**

- Pattern Recognition
- Activity Profiling
- Proactive and reactive surveillance techniques
- Planning Surveillance
- Hotspots
- Human Behaviour (Body Language, Suspicious Activity)
- Situational Awareness
- Incidence and Occurrences
- Lost contact Drills

**Selecting Subjects to view:**

- General viewing
- Known to the operator
- Previous criminal activity
- Body language (example squaring up to someone and stepping into their personal space)
- Request for assistance from another agency ie police etc

**Targeting and Tracking:**

- Using cameras to follow a particular person or vehicle
- Normally carried out if criminal activity is suspected
- Obtaining close up images

**The following rights of the public need to be considered when viewing:**

- Data Protection Act
- Human Rights Act
- If no criminal activity can be detected when zoomed in then the operator needs to zoom out and continue their camera patrol

**Image Sizes:**

- Images need to clearly identify the person in question
- A zoom of at least 120% needs to be used to positively identify someone
- The image needs to be clear and in focus
- If the images are to be used in identifying a particular crime, that also has to be clearly recognizable in the image

**Basic rule on image zoom sizes that can be used in evidence:**

- Identification - 100%
- Recognition - 50%
- Observation - 25%
- Detection - 10%
- Vehicles - 50%

Images can also be affected by frame rate, compression and low resolution

**Other things that can affect Image Quality:**

- Fog/mist
- Snow
- Obstructions (foliage, street signs, people or vehicles)
- Low Light

**Descriptions of People:**

- Ethnicity
- Gender
- Age (approx)
- Build
- Clothing
- Distinguishing Marks
- Height (approx)

- Hair
- Face
- Idiosyncrasies

If contact is lost also include last known location, direction of travel and when you last saw them

**Vehicle Descriptions:**

- Shape (Car, Van Etc)
- Colour
- Registration
- Identifying Marks
- Make
- Model

If contact is lost also include last known location, direction of travel and when you last saw the vehicle

**Actions to take when dealing with multiple incidents:**

- Work as a Team
- Prioritise
- Maximise use of equipment
- Communicate with team as well as partners

**Police Radio Links:**

- Most Town centre CCTV control rooms will have a dedicated radio link scheme in place with the police
- Radios are encrypted (Airwave is a system often used)
- Other schemes such as Town-Link (all shops have a radio link with the CCTV control room) and Pub-Link (all pubs, clubs and bars are linked to the CCTV control room) may also be in place

**Passing Information:**

- It is vital that all information is passed as quickly and efficiently as possible
- Delays may result in suspects escaping custody
- Delays can also result in lost eyewitnesses or evidence as well
- Always follow your local procedures for passing accurate information
- In serious incidents police should be notified immediately
- Remain professional at all times

# Different Types of Incidents and how to respond to them

**Incidents:**

- Any occurence that requires action to be taken by the CCTV operator

Operators can be made aware of incidents via the following:

- Reported by police directly to the control via a radio system
- Called in by a member of the public
- Pre-planned viewing of festivals/carnival events
- Operator views an incident while carrying out a patrol

Incidents could be **Emergencies**, **Urgent** or **Non-Urgent** in nature, all emergencies must be dealt with immediately and any assistance (police, emergency services) summoned right away.

**Non-Crime Incidents:**

- Evacuations
- Fire/Flood
- Traffic
- Crowds
- Street festivals
- Health and Safety issues
- Missing people

**Crime Incidents:**

- Theft
- Robbery
- Burglary
- Assaults
- Criminal Damage
- Drug Related

**Graded Response:**

- Immediate - Risk to life
- Routine - May need action
- Deferred

**Remember:**

- An operators job is to try to gather clear evidence/images of an incident
- An operator cannot stop the incident happening, however they can help the police with their investigations
- Operators may be able to contact the police directly to pass vital information to them live

**Crime and Disorder:**

- If operators are working in larger control rooms they should develop a good knowledge of their cameras and what areas they cover
- They should also get to know areas of increased criminal activity
- These areas may be different at different times of the day (nightclub entrances at closing time may be hotspots for public order offences)
- Larger operations will likely include liaising with the police and local authorities

**Crime Hotspots:**

- **Entrances to nightclubs** - fights
- **Crowded areas** - higher chance of pickpockets
- **ATMs** - Robberies and tampering with the machine
- **Alleyways** - poor lighting could lead to criminals using these to carry out crimes
- **Car Parks** - Car breaking and entering as well as thefts of motor vehicles
- **Train Stations** - fare evading, protection of staff and customers
- **Time of Day** - Rush hour versus quiet times may lead to different types of crimes

**Protection for Loan workers:**

- Regular check calls
- Visits to the control room to check up on loan workers
- Electronic devices, they can track movement for example

**Data Screen Regulations 1992:**

- Health and Safety law sets out how all the equipment in the control room should be handled and what safety measures should be in place to protect operators
- Ergonomic equipment should be used
- Chairs should be comfortable and promote sitting in the correct posture
- Screen breaks should be given to operators regularly, the law does not specify exact times though, screen time is usually broken up by doing paperwork or other jobs that do not involve looking at screens

**Risk Assessments:**

- All employers must carry out the appropriate risk assessments
- The assessments should cover each workstation
- Things to include would be screen size, distance and eye line
- Workstations should be adjustable and comfortable for the operator
- Operators should be trained on workstation setup

**Stress:**

- It is likely that operators will come across disturbing incidents as part of their job
- This may lead to stress
- Operators need to recognise when stress becomes a problem to their health
- Work related stress is the responsibility of an employer to have policies in place to provide support to minimise stress as much as is practical

**Symptoms of Stress:**

**Physical:**

- Headaches/Low energy
- Feeling drained
- Tense, muscular pain, back ache
- Rapid heart rate
- Chest Pain
- Insomnia
- Low immune system leading to getting ill more often

**Emotional:**

- Moody/agitated
- Feeling of being overwhelmed
- Constantly thinking about things without being able to switch off
- Low self esteem
- Avoiding others (even people that you are close to)

**Mental:**

- Racing thoughts
- Worrying all the time
- Unable to remain focused
- Forgetting things easily
- Bad judgement
- Only seeing the negative in situations

**Behavioural:**

- Procrastination, avoiding doing tasks
- Fidgeting
- Use of drugs and alcohol
- Changes in eating habits (eating more as a comfort or loss of appetite)

**Combating Stress:**

- Detach yourself from stressful situations
- Try to eat better food (control rooms can lead to bad eating habits)
- Try to exercise
- Go for walks or runs
- Try meditation techniques

**Taking Action against Hazards and Risks:**

- CCTV operators should report any hazards or risks that they spot outside or inside their control rooms
- If an operator takes no action against a hazard or risk that they have spotted this could lead to legal action against them if someone is hurt or killed as a result

**Hazards that an Operator may face in the control room:**

- Fire
- Bomb Threats
- Trip slip hazards
- Electrical hazards

**PRACTICAL USE**
OF CCTV EQUIPMENT

**Suspicious Activity:**

- Ensure that recording is started (most modern systems record constantly so this may not be required)
- Zoom in to get as much detail as possible
- If people are running it may be easier to track them by zooming out to keep them in frame
- Know your camera map so you can switch cameras for better views

**Image Size:**

- Remember to take into account The Human Rights Act and the respect for their privacy
- Operators need to be able to justify recording identifiable images

**Dealing with Multiple incidents:**

- Operators need to decide which incident needs priority when multiple incidents occur simultaneously

**Priority order:**

1. Risk to life
2. Risk of serious injury
3. Loss of evidence
4. Loss of or damage to property

**Always remember:**

- Communicate
- Prioritise
- Use communication channels (radios, phones etc)
- Make notes
- Work as a team
- Write accurate reports

**Body Language:**

- A lot of CCTV systems will record visuals only and may not have an audio function
- Operators will need to rely on people's body language and behaviour instead
- Body language is non-verbal communication (not words or tone)
- Operators need to try to develop their body language reading skills

| Body Language | Possible Meaning |
|---|---|
| Walking quickly with head up | confidence |
| Hands on hips | Possible confrontational stance |
| Crossed arms on chest | Blocking and defensive attitude |
| Hands in pockets and head down | Dejected |
| Hands above shoulder height | Signs of stress |
| Stepping into another person's personal space | Confrontational, possibility of violence |
| Open palms | Sincerity |

**Control Room Procedures:**

**Start Of Shift:**

- Shift handover should be thoroughly checked, preferably before the other shift manager has left incase there are any questions
- Work stations set up
- Radio checks carried out
- Operators must always carry out a full system check when starting a shift to make sure all systems and cameras are working properly
- Any faults should be reported

- Operators may have trouble shooting techniques to rectify smaller issues
- Any fault reporting paperwork should be complete
- Control room diary should be checked for any upcoming events

**You will be assessed on the following as part of your CCTV Qualification:**

- Use of equipment
- Tracking
- Searching for objects
- Image sizing for evidence (120 % zoom for identification purposes)
- How to record
- How to produce evidence
- Completing audit trials
- Dealing with environmental issues (low sun in the lense, obstacles in the way etc)
- Report writing

**ADDITIONAL RESOURCES:**

**https://www.gov.uk/government/news/act-awareness-elearning**

**Mock Exams**

Scan the QR Code to access mock exams.

## BECOME CERTIFIED SECURITY PROFESSIONAL

The Get Licensed Certified Security Professional status is a mark of recognition for front-line security professionals who have completed a varied of front-line training to a superior standard.

**Earning Criteria:**

- Door Supervisor Training / Security Officer Training
- CCTV Training
- Emergency First Aid at Work
- Basic Handcuff Training

To learn more about Certified Security Professional scheme, scan the QR code:

## Have a valid SIA licence? Create your Get Licenced security worker passport today and Get Working.

### Sign Up

Give us your details and we'll run some quick checks  to activate your account

### Get Notified

Get notified of new matching opportunities in your area.

### Select Shift

Apply for shifts to suit your schedule and work around your availability.

### Get Paid

No more waiting for payday, get paid the same day after completing your shift.

# I CURRENTLY DO NOT HOLD AN SIA LICENCE, HOW DO I GET ONE?

1 Register

**Register for a personal online account**
**1.** Enter personal details and email address
**2.** Choose username and password
**3.** You will receive an activation email. Click the link in the email to activate your account

If you do not receive the activation email please check your trash folders

2 Log In

**In SIA's self service website**
**1.** Enter username and password
**2.** Enter requested information on the ‘match your details’ page
**3.** If you held a licence in the past this will match your new account with existing licence information we hold

Your login credentials from our old site will not work

3 Apply

**When logged into your online account**
**1.** Click ‘Start a New Application’ or Click the ‘Licences’ tab and ‘Actions’, ‘Renew’
**2.** Complete sections 1-9
**3.** Review and submit your application

A record of your qualifications should be present, if not contact your training provider

4 Next steps

**You will receive a notification in your online account and an email to explain your next steps**
**1.** If you are applying for a licence for the first time, when instructed visit a post office to have your ID documents checked and photo taken
**2.** If you are renewing your licence and your photo has expired (lasts 5 years 8 months) you will be instructed to visit a post office to have your photo taken
**3.** You may receive an email asking you to send additional documents to SIA (overseas criminality record or passport)

SIA needs to complete and approve all ID checks and have received payment for your licence before you move out of Next Steps

5 Checks in Progress

**SIA checks your criminal record, right to work and photographs**
SIA may email you asking you to send additional documents related to these checks

Responding promptly to requests for further information will help speed up the processing of your application

Check the status of your licence application at any time in your online account

6 Decision

**You will receive a decision notification in your online account and via email**
- Decision to grant: you will receive a granted letter and your licence card will follow within 14 days
- If SIA proposes to refuse your licence application SIA will write to you to explain why; you will have 21 days from the date on our decision letter to provide a response

As soon as you receive confirmation that your licence has been granted, you can lawfully work. Please print your licence number as it appears on the Register of Licence Holders and carry this with photo ID

We would like to thank you for taking this step and join the UK's Security Industry - we can't wait for you to get started.

The world needs virtue more than ever. We need heroes. We need those who stand up for the common good, no matter what the circumstances.

Always remember, If you act virtuously - everything else important could follow: Happiness, success, meaning, reputation, honour, love.

**We hope that you never forget to do the right thing!**

**GET LICENSED** is the UK's leading training and staffing platform for security workers. Founded in 2007, with a vision to serve the security industry - the company has helped over 300,000 individuals launch their career in the Security Industry and provides a fully integrated staffing solution to security companies of all sizes.

Visit get-licensed.co.uk and ***Get Working with Get Licensed.***

GET
LICENSED

get-licensed.co.uk