© 2021 Highfield Products Limited

Tutor guidance and general advice

- Carefully study the training pack and ensure that you are familiar with its contents.
- On this first slide, enter your name in the space provided. The date will update automatically.
- Ensure you have a full set of training aids to enhance your lecture.
- Include any additional aids you intend to use with the list provided.
- Add the visual aids and examples of group exercises, handouts, newspaper articles, anecdotal stories and jokes you intend to use at the relevant page of each of these notes. Any omissions or new information you wish to include in the lecture should also be added.

- Group work and interactive sessions are an essential feature of any successful

course. Several examples are included with the pack.

- Ensure that there are adequate strategically timed breaks and always finish on time.

- Lecturers should arrive at least 30 minutes prior to the lecture to check:

    - All equipment is working satisfactorily, that they know how to operate it and participants can clearly see and read the information projected

    - The projector is properly focused and the screen is clearly visible from all parts of the room; ensure it is safe and there are no trip hazards caused by wires. It is also useful to have a spare bulb and to know how to change it.

    - The lecture room is arranged to suit the style of lecture and the visual aids being used.

- The PowerPoint™ slides in this pack will enhance your lecture.

- Always face the audience when speaking and do not address your comments to the screen, with your back to the participants.

- If you have any suggestions for improving this training pack or would like any specific amendments, please do not hesitate to contact Highfield on 01302 363277.

Good luck with your course.
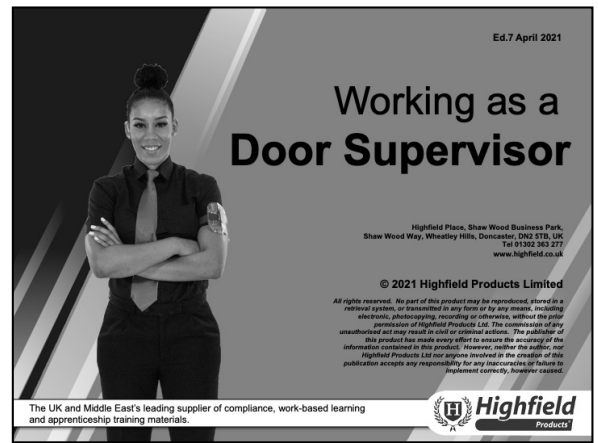
Module 1: Principles of working in the Private Security Industry

This training presentation covers the learning outcomes and assessment criteria for unit 1: Principles of Working in the Private Security Industry (level 2 Award for Door Supervisors in the Private Security Industry qualification).

Module 2: Principles of working as a door supervisor in the private security industry and Module 3: Application of conflict management in the private security industry are provided as 2 separate training presentations included in this training package (3 training presentations in total).

- **A family-run business, employing over 250 staff worldwide, including internationally recognised subject matter experts**
- **Over 2 million people are trained every year using Highfield products**
- **Over 20,000 trainers and approved centres deliver Highfield qualifications**
- **A client list comprising the world's most recognisable organisations in their field**
- **Internationally recognised accredited qualifications.**

Everything we do centres around our core values of:

- **quality** - leading international industry experts from all fields, with supporting training materials available from Highfield
- **value** - we will not be beaten on value. We concentrate on the areas important to our clients, including dedicated customer support, exceptional supporting documentation and unbeatable service and turnaround times
- **service** - we provide all of our centres with their own dedicated account manager and have a turnaround time of 4 working days for results and certification
- **integrity** - we provide our centres with accurate and honest information at all times - we never put profit before good advice.
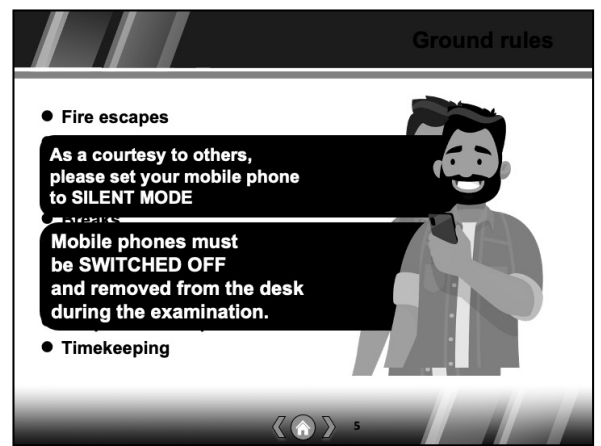
This can be made interactive by encouraging delegates to suggest ground rules.

Examples may include:

- confidentiality/anonymity or at least not mentioning names
- being open
- participating
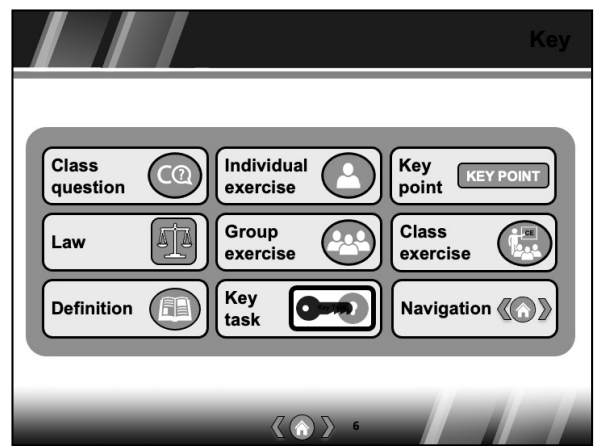
The above symbols are primarily for tutors so that you know when a class question or exercise may be appropriate.

1	Module 1: Principles of working in the private security industry
2	Module 2: Principles of working as a door supervisor in the private security industry
3	Module 3: Application of conflict management in the private security industry
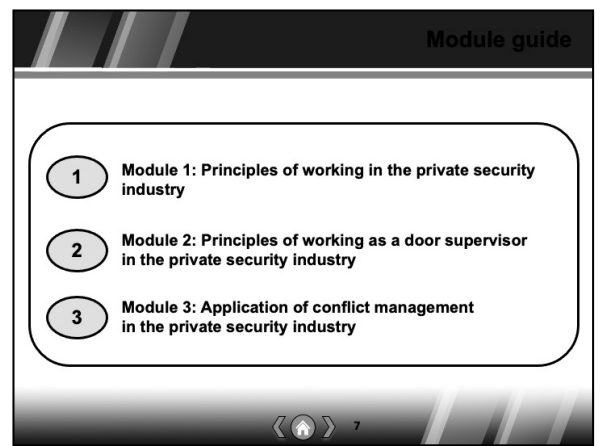
This training presentation includes module 1: Principles of working in the private security industry.

Module 2: Principles of working as a door supervisor in the private security industry and Module 3: Application of conflict management in the private security industry are provided as 2 separate training presentations included in this training package (3 training presentations in total).

Principles of working in the private security industry
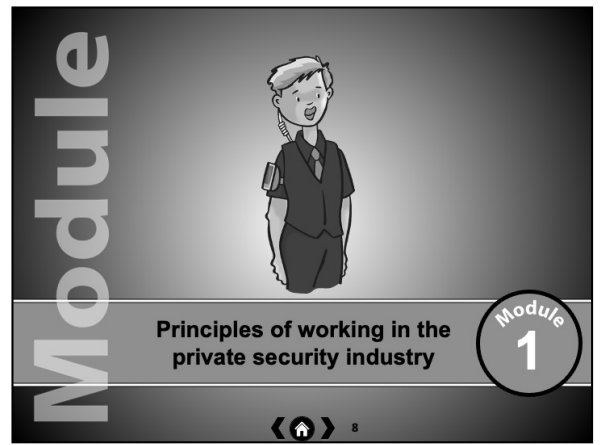
Module 1

This module covers:

- the private security industry
- legislation
- arrest procedures
- safe working practices
- fire procedures
- Emergencies
- communication skills
- record-keeping
- terror threats
- vulnerable people
- post-incident management

This module covers:

1:1 the private security industry

1:2 legislation

1:3 arrest procedures

1:4 safe working practices

1:5 fire procedures

1:6 emergencies

1:7 communication skills

1:8 record-keeping

1:9 terror threats

1:10 vulnerable people

1:11 post-incident management.

- 11 modules in total
- Comprehensive tutor notes
- Class discussion topics and class questions
- Key tasks at the end of each module should be answered by all learners simultaneously to ensure everyone understands before moving to the next module.

The private security industry

Module 1:1

Completion of this module will enable learners to meet the following learning outcome:

Learning outcome 1: Know the main characteristics and purposes of the Private Security Industry

This includes assessment criteria:

1.1 Identify the key purposes of the private security industry

1.2 State the aims and functions of the Security Industry Authority (SIA)

1.3 Recognise the required standards of behaviour of a security operative

1.4 Identify the benefits of community safety initiatives

1.5 Recognise how assignment instructions support the Security Operative role

1.6 Recognise how each security operative role may use CCTV

1.7 Identify the limitations of CCTV within the security operative role

1.8 State the purpose of the Approved Contractor Scheme

This module includes the following interactive activities:

• class question: What is security?

• class question: What qualities do you think security operatives should posses?

• class question: What are the legal implications of using CCTV?

Key task 1

Security is a state or feeling of being safe and secure

'providing services to protect premises, people and their property'.

11
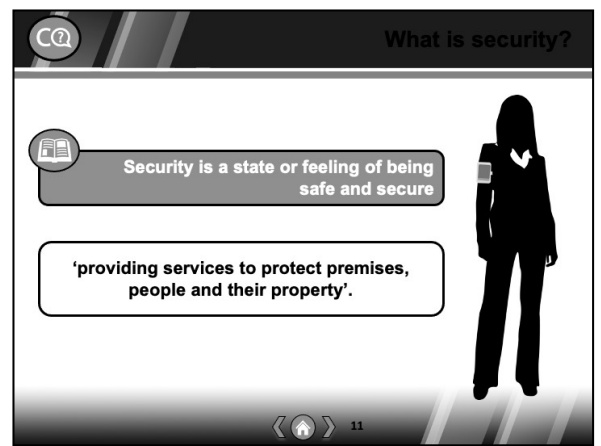
Class question: What is security?

Click to reveal the answer.

The security industry is required to be regulated due to unscrupulous companies and criminal gangs forcing themselves upon businesses.

911 also had an impact as countries worldwide examined their security vetting procedures to prevent terrorists and other unauthorised people being able to carry out such a devastating act again.

The Private Security Act 2001 was not implemented until 1 January 2003 on a roll-out basis across the UK, starting with London. It was implemented into all areas of the UK by 1 January 2004.

Main aims of security

- Prevent and detect crime
- Prevent or reduce loss, waste and damage
- Monitor and respond to safety risks.

- Prevent by visual deterrent and detect crime through observation and possibly coordination with CCTV operative.

- Prevent and reduce loss via monitoring staff and customers to reduce theft. Turning off lights etc. reduces waste.

- Knowing how and responding appropriately to safety risks.

Security can be provided to clients in 3 main ways:

- manned security
- physical security
- systems.

Security can be provided to clients in 3 main ways:

- manned security – where 1 or more security operatives (male or female) work on a site, providing both a deterrent against crime and an immediate response to incidents as they occur
- physical security – physical deterrents such as locks, alarms, barriers and grills to help reduce crime
- systems – electronic and other technical systems to monitor premises for crime and other dangers such as intruder alarms, fire detection systems and closed-circuit television (CCTV) systems

Some systems are a combination of physical security and systems e.g. an intercom with image and magnet lock.

The SIA has 3 main aims:

the compulsory licensing of individuals undertaking designated activities within the private security industry

to recognise quality service by managing the voluntary Approved Contractor Scheme (ACS)

to introduce business licensing for all regulated security companies.

14
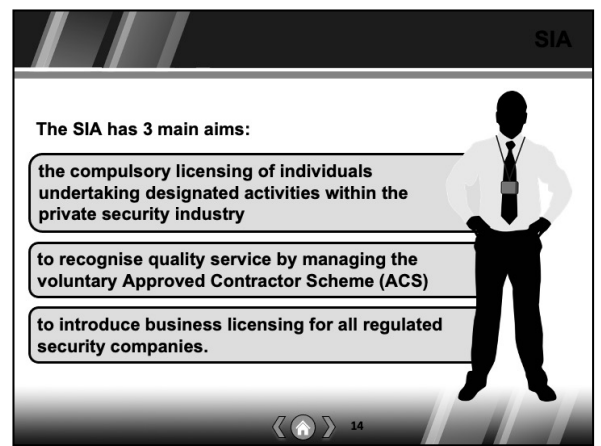
This is a good point at which to mention the Private Security Act 2001 http://www.legislation.gov.uk/ukpga/2001/12/contents. This is covered in more detail later.

Directly employed CCTV and security officers (guards) are not regulated by the SIA.

ACS is a voluntary scheme that companies pay for. It is an accreditation from the SIA, stating that all procedures, including record-keeping, meet or exceed the SIA standards. These companies do not need to wait for an SIA licence to arrive prior to employing a security officer. They are allowed 10% of their employees to be in the process of being licensed by the SIA for up to 16 weeks.

Business licensing will standardise company record-keeping and insurance. There is currently no date for implementation of this scheme (January 2020).

Approved Contractor Scheme (ACS)

Designed to raise standards of security companies

These companies will assist the SIA with developing new opportunities

Increases customer confidence in the private security industry.

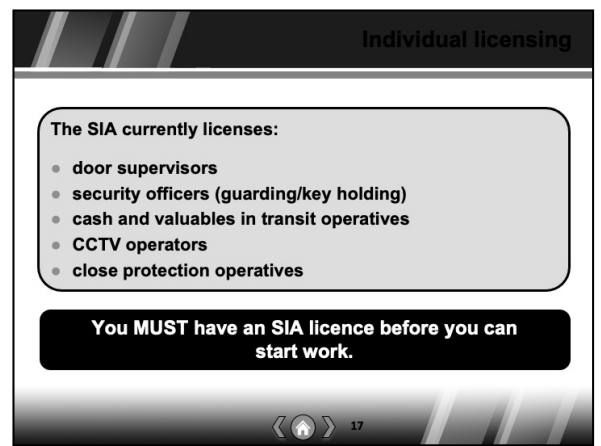The ACS introduced both operational and performance standards for private security companies.

Only companies that can prove they can meet the ACSs high standards will be awarded 'Approved Contractor' status.

The SIA's main functions are to:

- protect the public and regulate the security industry through licensing
- raise standards (through the Approved Contractor Scheme)
- introduce business licensing for all regulated security business
- monitor the activities and effectiveness of those working in the industry
- set and approve standards of conduct, training and supervision within the industry
- keep under review the private security industry and the operation of the legislative framework
- increase customer confidence

The SIA currently licenses:

- door supervisors
- security officers (guarding/key holding)
- cash and valuables in transit operatives
- CCTV operators
- close protection operatives

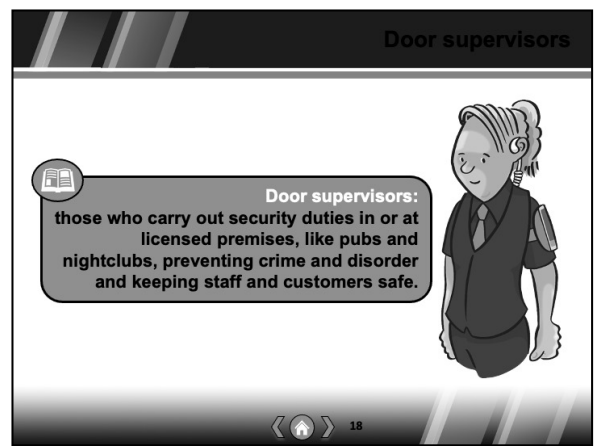**You MUST have an SIA licence before you can start work.**

Individual licensing

Anyone wishing to work as a security operative must have an SIA licence before they start work. This is covered in more detail under 'individual licencing' further in this training presentation.

- Licensed sectors in all of the UK

- Northern Ireland also includes vehicle immobilization. These are security operatives who either remove or relocate vehicles, restrict the movement of vehicles using a device or release vehicles after demanding or collecting a charge

Other as yet non-regulated sectors of the private security industry include private investigation, event security, electronic security and fire systems.

Door supervisors: those who carry out security duties in or at licensed premises, like pubs and nightclubs, preventing crime and disorder and keeping staff and customers safe.

Door supervisors - those who carry out security duties where alcohol is being consumed.

This SIA licence also includes the duties of a security and retail officer. Many people with this licence do not work stereotypical venues such as night clubs but may require this licence to work an event with a bar.
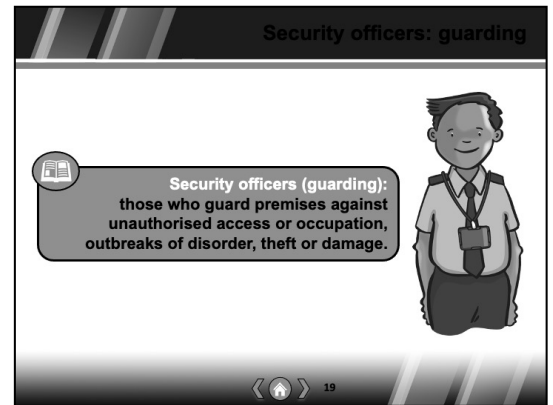
Security officers (guarding) – this sector includes providing security at factories, retail premises, building sites and hospitals - in effect, anywhere that alcohol is not being consumed. It also allows the individual to work at an off-licence (e.g. supermarket) as alcohol is only being sold, not served.

Security officers (guarding) may also guard individuals against assault/injury as the result of the unlawful conduct of others.

They can either provide physical protection or protection by way of patrolling or surveilling, thereby deterring crime.

Key holding
Key holding is where a security officer keeps custody of, or controls access to, any key or similar device for operating (whether mechanically, electronically or otherwise) any lock.

Key holding is not a specific license but is an SIA-regulated sector. Someone who locks/unlocks or responds to an alarm activation is required to hold either a door supervisor or security officer SIA licence. This does not apply to an individual such as a caretaker in a school who is employed directly by the company who owns/rents the premises.
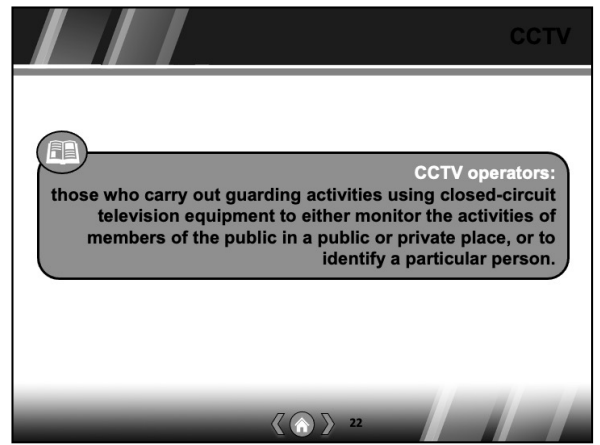
Key holders do not provide security themselves, they simply hold the keys for the company.

Cash and valuables in transit operatives will operate secure machinery, for example money vans.

> **CCTV operators:**
> those who carry out guarding activities using closed-circuit television equipment to either monitor the activities of members of the public in a public or private place, or to identify a particular person.

A CCTV operator's role includes watching live images and reviewing footage not including themselves. It also includes reviewing images from body-worn cameras.

This does not apply to individuals employed directly by the business but is an additional licence for all contracted security operatives. Anyone can review footage that includes themselves for the purpose of accurately writing an incident report.

Close protection operatives: those who guard one or more individuals against assaults or injuries that might be suffered as a consequence of the unlawful conduct of others.
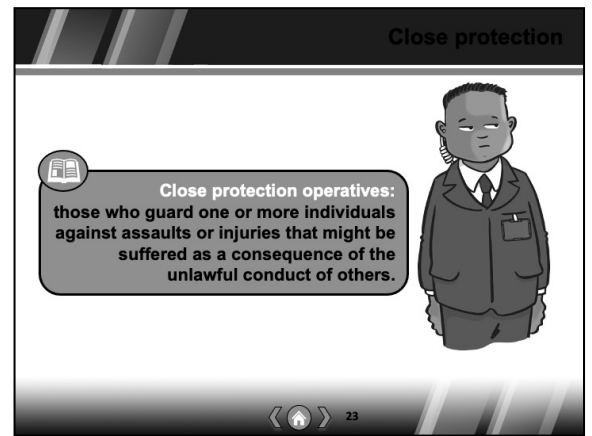
Close protection operatives are commonly called bodyguards.

Their roles may include protecting people or property.

This is currently (January 2020) the only SIA licence that would also allow the holder to work in the door and security officer sectors.

Vehicle immobilisers:
security operatives who either
remove or relocate vehicles, restrict
the movement of vehicles using a
device or release vehicles after
demanding or collecting a charge
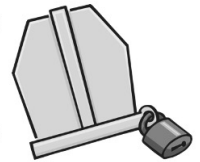
BUT - only licensed by the SIA in Northern Ireland.

24

Vehicle immobilisers are only licensed by the SIA in Northern Ireland. These are security operatives who either remove or relocate vehicles, restrict the movement of vehicles using a device or release vehicles after demanding or collecting a charge.

Licensing ensures that security operatives are:

- 'fit and proper' persons
- properly trained and qualified to do their jobs

The SIA sets standards of conduct, training and supervision within the industry.

25

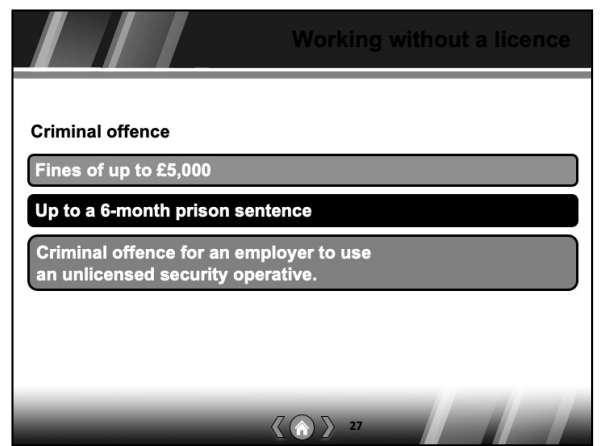Licensing ensures that security operatives are 'fit and proper' persons who are properly trained and qualified to do their jobs.

Fit and proper is not just a physical limitation but also refers to the operator's mental state e.g. is it a good idea to work a shift directly after someone close to you has died?

Anyone wishing to work as a security operative must have an SIA licence before they start work.

- Apply to the SIA itself
- Your identity will be verified
- Specified training must be undertaken
- Your criminal record will be checked
- A license fee will be payable
- Licence will last for 3 years before renewal.

An individual will need to set up an account on the SIA website (https://www.sia.homeoffice.gov.uk/Pages/licensing-applying.aspx). Once set up, an employer can link to it and complete the application on the individual's behalf, or the individual can complete it. Once submitted, it will message the applicant telling them their reference number and which documents to take to the approved post office. They must present their application reference number and the documents. The post office will take the payment and their photograph.

Criminal offence

Fines of up to £5,000

Up to a 6-month prison sentence

Criminal offence for an employer to use an unlicensed security operative.

27

Anyone wishing to work as a security operative must have an SIA licence before they start work, unless working for an ACS-approved company.

It is the legal responsibility of the security company, and the business they send you to work for, to check that your SIA licence is valid. This can be done on the SIA website.
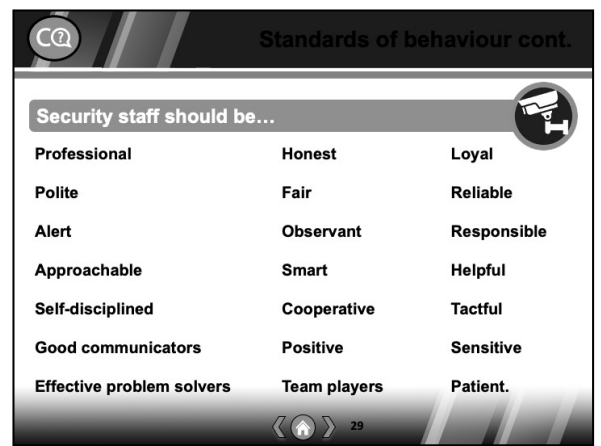
Standards of behaviour

Security operatives must always conduct themselves professionally as clients/members of the public expect them to display certain standards of behaviour

What qualities do you think security operatives should possess?

28

Class question: What qualities do you think security operatives should posses?

Answers are on the next slide. You may consider taking answers in an open format or on a flip chart.

Standards of behaviour cont.

Security staff should be…

Professional	Honest	Loyal
Polite	Fair	Reliable
Alert	Observant	Responsible
Approachable	Smart	Helpful
Self-disciplined	Cooperative	Tactful
Good communicators	Positive	Sensitive
Effective problem solvers	Team players	Patient.

29

Answers

Discuss why these qualities apply to a security operative, for example 'smart' relates to a security operative's appearance and being 'loyal' could suggest that they would arrive for their shift even if a different venue offered them a slightly higher pay rate an hour before their shift was due to start.

Could also mention the following traits:

- sensitive
- responsible
- courteous
- handle sensitive situations

If learners mention traits other than those above, discuss why/if they apply to security operatives.

Above all security operatives should have integrity and be prepared to take responsibility for their action.

Security operatives MUST always conduct themselves:

in strict accordance with the SIA's Code of Behaviour for their particular role within the industry

according to their own organisation's values and standards.

The SIA Code of Behaviour is available on the SIA website but the contents of it are explained during this course.

- Improving the physical security of vulnerable areas
- Improve the environment
- Removing the means and opportunities to commit crime
- Provide funding for extra lighting and CCTV Communal radio systems
- Pubwatch/Shopwatch initiatives
- Warning signs
- Using CCTV
- Using the yellow and red warning cards.

Encourage learners to research what is available in their areas.

Local authorities now use Safer Community Partnerships to help reduce crime and the fear of crime in their areas. They work together with the police, the other emergency services and other relevant public and private organisations

to try to reduce crime, public disorder, reoffending, anti-social behaviour, substance misuse and vandalism.

Crime reduction initiatives try to do this by:

- improving the physical security of vulnerable areas

- improving the environment itself

- removing the means and opportunities to commit crime

- using extra lighting to improve visibility in an area

- using warning signs

- controlling access to certain areas at specific times

- using CCTV

- using radio communications between various organisations and companies

- making use of local and national Pubwatch and Shopwatch initiatives

- using the yellow and red warning cards in conjunction with the local Pubwatch policy

Aims of crime reduction initiatives

To try to reduce:

- crime
- public disorder
- reoffending
- antisocial behaviour
- substance misuse
- vandalism/graffiti.

32

The main aims of local crime reduction partnerships are to reduce crime, public disorder, reoffending, antisocial behaviour, substance misuse and vandalism.

Assignment instructions (A.I.s)
These are a set of written guidelines on what needs to be done and how it should be done on that particular site

Complying with these instructions will ensure you stay within the law and the client's requirements.

A.I.s

33

Assignment instructions - A.I.s

Describe in detail the security operative's activities for each site, emergency procedures and contact numbers.

This term is not usually used in licensed premises but is primarily used in static premises, including building sites, factories, retail etc.
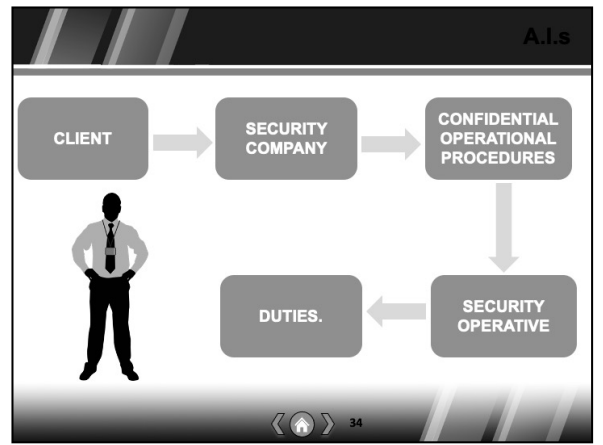
Flow diagram of how A.I.s are created and used.

A.I.s cont.

A.I.s contain details and instructions on:

- duty times
- site plans
- site risks
- location of high-value property
- areas of vulnerability
- patrol times/routes
- access/egress procedures
- search procedures
- reporting procedures
- health and safety issues
- first-aid procedures
- methods for calling the emergency services
- important contact telephone numbers
- emergency and evacuation procedures
- alarm/surveillance systems
- methods of communication
- relevant documents.

A.I.s will contain details and instructions on each item included on the slide.

- **Always read the A.I.s when you start on a new site**
- **Keep yourself up to date with the contents**
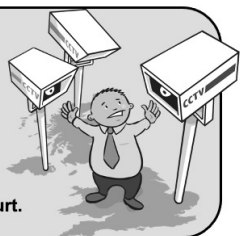- **You may need to sign a form confirming that you have read the A.I.s at the start of each shift**

A.I.s are CONFIDENTIAL documents – keep them secure.

A.I.s are **CONFIDENTIAL** documents and must be kept securely so that unauthorised people do not have access to them.

Benefits of using CCTV

- Prevents crime
- Reduces incidents
- Reduces costs/risks by not having to employ additional patrolling staff
- Can provide clear evidence for investigations
- Can be used as evidence in court.

CCTV does not prevent crime but the learning outcome and therefore exam questions may state this.

There are many benefits that come with using CCTV, for example:

- CCTV does deter some people from committing a criminal act.

- it can reassure customers/staff of their safety

- monitoring CCTV is safer than actually patrolling a site and monitoring multiple screens at once can allow you to observe a site quicker than if you were to walk around it. As there is less risk to the security operative, there is therefore less time off sick after incidents/accidents and no compensation claims if injury occurs during a physical patrol.

There are also disadvantages of using CCTV, for example:

- the evidence obtained from CCTV is only good if the system meets requirements and has sufficient coverage

- blind spots could adversely affect the chain of evidence if footage does not adequately prove or disprove guilt

- poor quality images may not be admissible in court

Class question: What are the legal implications of using CCTV?

- CCTV systems should ideally be monitored at all times and must be registered for an approved use, e.g. health and safety and security
- The accountable person is the data controller
- Signage must state the approved purpose, who is operating the system (data controller's name or company name), contact number for queries about the system and subject access requests (copies of footage involving the person requesting the copy)

- The ICO approval includes the declared time that footage can be retained on the system before it over-records
- Approved list of who can access the CCTV system known as 'authorised persons'
- Recordings must be used appropriately.

39

The maximum time that footage can be retained on the system is usually 28 days; this does vary but must be justified.

The general review of live footage must be done by trained and authorised people only, e.g. human resources cannot view CCTV to verify staff performance without the permission of the employees.

Must only record for the purposes that are stated in the ICO approval.

- Privacy issues and concerns
- Vulnerable to damage and vandalism
- Misuse
- Cannot prevent crime
- Cost
- Familiarity with scope of cover
- Technology vulnerabilities.

There may be some limitations of using CCTV, for example:

- some people do not like being recorded as they feel it violates their privacy
- incorrectly positioned cameras may be damaged (they should be positioned well above head height to avoid this)
- operative misuse
- some people will wear items to cover their face
- initial cost can be prohibitive
- an operator's ability and knowledge of how to use the equipment - do they know where the blind spots are?
- wireless signals can be disrupted, and cables can deteriorate over time
- it may be misused for the unauthorised monitoring of people (illegal in many cases)

1 What does the abbreviation SIA stand for?

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

1 **What does the abbreviation SIA stand for?**

Security, Industry, Authority.

② **Describe the THREE main aims of the SIA.**

1 ....

2 ....

3 ....

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

2 Describe the THREE main aims of the SIA.

1 Protect the public and regulate the security industry through
licensing

2 Monitor the activities and effectiveness of those working
in the industry

3 Set and approve standards of conduct, training and supervision
within the industry.

③ Identify FIVE standards of behaviour expected of a security operative.

1 ....

2 ....

3 ....

4 ....

5 ....

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

3 Identify FIVE standards of behaviour expected of a security operative.

1. Professional
2. Polite
3. Honest
4. Observant
5. Approachable.
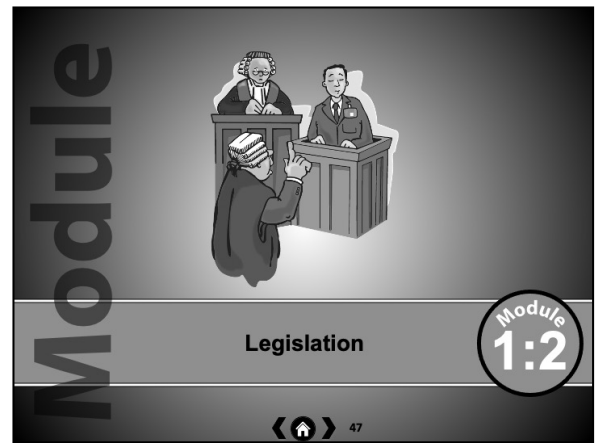
Completion of this module will enable learners to meet the following learning outcome:

Learning outcome 2: Understand legislation as it applies to a security operative

This includes assessment criteria:

2.1 Identify the differences between Civil and Criminal Law

2.2 State the main aims of the Private Security Industry Act 2001

2.3 Identify key legislation relating to promoting equality and diversity in the workplace

2.4 Identify licensable roles under the Private Security Act

2.5 Identify how data protection regulation impacts on the security operative

 This module includes the following interactive activities:

Key task 2

Civil laws usually deal with disputes between people, companies or other organisations

They deal with things like:
- libel
- slander (known as defamation in Scotland)
- personal injury cases
- trespass.

Civil laws help govern our daily lives.

Civil offences:

- themselves do not occur a potential prison sentence
- Civil cases are usually dealt with in the county courts, with more serious cases being heard in the High Court. In Scotland, civil cases are heard by the

  Sheriff Court with more serious cases being heard at the Court of Session.

Other cases dealt with under civil law include:

- family and matrimonial disputes
- personal injury cases
- employment law
- breach of contract

The standard of proof is 'on the balance of probabilities'.

49

Civil laws help govern our daily lives.

Other cases dealt with under civil law include:

- family and matrimonial disputes

- personal injury cases

- employment law

- breach of contract

Ensure that you emphasise that the standard of proof in the civil court is 'on the balance of probabilities'.

Trespass:
A trespass is committed by a person who is improperly on someone else's property without consent.

Trespass:
- is not normally a criminal offence
- can be actionable through the civil courts
- is an act of interference against the 'lawful occupier'.

The act of trespass is being somewhere without permission and is itself classed as a civil offence, however it may be coupled with an indictable (criminal) offence such as threats to harm or criminal damage.

The '**lawful occupier**' is someone who owns, occupies or has control over the property, for example the owner, manager or person in charge of the premises or any member of staff acting on their behalf, including a security operative.

Examples of trespass include:

- refusing access to a shop as it is due to close, but the person still walks into the shop

- gaining entry to a site through a hole in the fencing even if the trespasser did not create the hole

- asking someone to leave licensed premises and the individual not complying with the request

Scotland

The Trespass (Scotland) Act 1865 makes it an offence under Scots law to trespass.

Trespass in licensed premises in Scotland

Under Section 116 of the Licensing (Scotland) Act 2005 it is an offence for any person to refuse to leave licensed premises as follows:
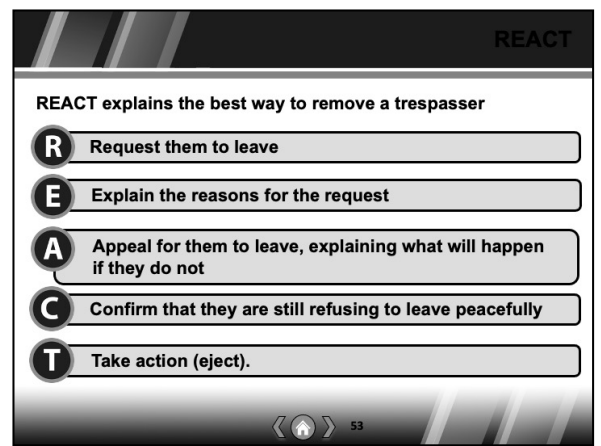
- a person on any relevant premises who behaves in a disorderly manner,

- and refuses or fails to leave the premises on being asked to do so by a responsible person or a constable, commits an offence

- a person on any relevant premises who, after the end of any period of licensed hours, refuses or fails to leave the premises on being asked to do so by a responsible person or a constable commits an offence

Northern Ireland

In relation to trespass, the new criminal trespass law enacted under s128 of SOCPA, has made it illegal to trespass on certain designated military and nuclear sites in Northern Ireland. There is a common law offence of trespass against property and a criminal law offence of trespass/harassment against the person, including assault.

Security operatives may ask people to leave a premise if they:

have no reason to be there

break criminal laws

break licensing laws

breach specific premise rules or conditions

start to display unacceptable behaviour.

REACT explains the best way to remove a trespasser

R   Request them to leave

E   Explain the reasons for the request

A   Appeal for them to leave, explaining what will happen if they do not

C   Confirm that they are still refusing to leave peacefully

T   Take action (eject).

REACT is a model for when someone has accessed your premises and you are requesting them to leave.

A good exercise for the group could be to slightly amend the model to one for refusing entry, for example:

- R - request the person not to enter
- E - explain the reasons for the request
- A- appeal for them to not attempt to enter explaining what will happen if they do attempt to enter
- C - confirm they still intend to enter
- T - take action (close the door, block their entry path etc.)

- Criminal laws are in place to prevent people from committing more serious offences and to punish people when those laws are breached
- Offences are usually committed against people or property
- Cases are normally brought by the state
- Guilty verdicts can result in fines, probation orders and terms of imprisonment
- The standard of proof in the criminal courts is 'beyond reasonable doubt'.

54

Criminal laws come from either:

- very old judicial decisions made in courts (common law)
- Acts of Parliament (statute law)

Cases are normally brought by the state, often following an arrest.

Prosecution is sought through the criminal courts.

Emphasise that a criminal offence may result in imprisonment and possibly a fine.

The standard of proof in the criminal courts is 'beyond reasonable doubt' due to potential to take away a person's liberty.

This slide has the potential for a discussion about whether juries are really objective in modern times as most cases are described on social media or the news. Can a modern day jury really not have any preconceived ideas about what happened?

Serious crimes include:

Serious crimes include:

- murder - intentionally killed another person
- rape – insertion of penis without permission into anus, mouth or vagina
- ABH – actual bodily harm – cuts, bruises and broken nose
- GBH – grievous bodily harm – broken bones etc.
- GBH w/i – grievous bodily harm with intent – planned breaking of bones etc.
- sexual assault – physical/psychological/emotional violation in the form of a sexual act, imposed on someone without their consent
- drugs is referring to illegal drugs e.g. cocaine, heroin etc.
- theft – stealing an item
- fraud – misappropriating money or an item by the means of deception e.g. pretending to be a builder, taking the deposit and then never going to complete the work paid for
- robbery – the act of theft but with a person involved e.g. robbing a bag
- burglary (housebreaking in Scotland) - entering premise with the intention to steal
- arson (wilful fire-raising in Scotland) – deliberately setting fire to something with the intention to cause damage
- threats to harm and or damage, child and domestic abuse are as per their titles
- kidnapping – consider arresting the wrong person as well as general kidnapping

The Private Security Industry Act

As well as the above, the Private Security Industry Act also intended to remove criminal elements from the private security industry and established licensing of individuals.

http://www.legislation.gov.uk/ukpga/2001/12/contents

The act allows the SIA to:

- license individuals in specific sectors
- approve security companies
- monitor the activities and effectiveness of those in the industry
- remove criminal elements from the industry
- keep the industry under review
- conduct inspections
- set standards of training and supervision
- make recommendations to improve standards.

A prejudice is a hostile attitude towards someone who belongs to a certain group, simply because they belong to that group, and are therefore assumed to have all of the characteristics ascribed to that group

Stereotyping is when we lump certain groups of people together, assuming that they are all the same simply because they belong to that group.

The Equality Act 2010

58

Equality and diversity in the workplace

The SIA is only concerned with our negative prejudices.

The Equality Act prohibits discrimination based on:

- age
- disability
- gender reassignment
- marriage and civil partnership
- pregnancy and maternity
- race
- religion
- sex
- sexual orientation

Known as 'protected characteristics'.

The Equality Act

These are known as protected characteristics.

Larger companies must now monitor the ratio of genders and ensure all are being treated equally, regardless of gender or protected characteristics.

protected characteristics.

Northern Ireland

In Northern Ireland, discrimination is illegal under the following laws:

• The Race Relations (Northern Ireland) Order 1997

• The Sex Discrimination (Northern Ireland) Order 1976

• The Disability Discrimination (Northern Ireland) Order 2006

As a security operative, you cannot refuse entry or evict anyone on the grounds of sex, race, colour, disability or physical appearance. Should you refuse entry to or evict an individual for any of these reasons alone then you will be committing an offence. The individual who has been discriminated against has the right to make a formal complaint to the premises management requesting an apology, a commitment that such discrimination does not reoccur or even compensation. If the issue is not dealt with to their satisfaction, they may even take legal action against you and your employer.

The Equality Act also applies to:

- recruitment
- access to training
- pay and benefits
- promotion opportunities
- terms and conditions
- redundancy
- dismissal
- making reasonable adjustments
  for employees with specific needs/disabilities.

60

The Equality Act

It is illegal for employers to discriminate against any of these groups of people in the areas of recruitment, access to training, pay and benefits, promotion opportunities, terms and conditions, redundancy and dismissal.

Furthermore, employers now have to make reasonable adjustments to cater for the employment of disabled people.

Direct discrimination occurs when someone is treated less favourably than another person because of a protected characteristic they have or are thought to have, or because they associate with someone who has a protected characteristic
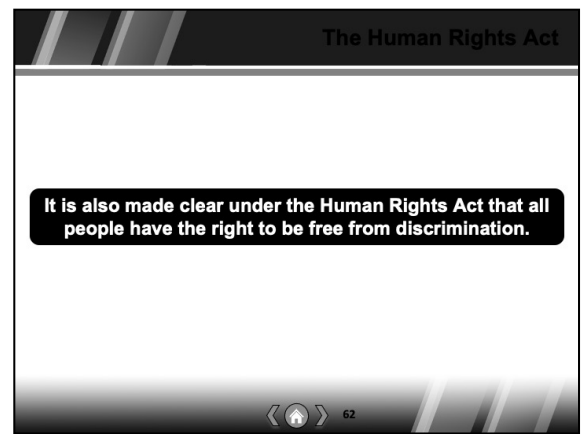
Indirect discrimination occurs when a policy or practice that applies to everyone particularly disadvantages people who share a protected characteristic.

61

Types of discrimination

- **Direct discrimination** occurs when someone is treated less favourably than another person because of a protected characteristic they have or are thought to have, or because they associate with someone who has a protected characteristic.

- **Indirect discrimination** occurs when a policy or practice that applies to everyone particularly disadvantages people

Discrimination can be hurtful, insulting and demeaning to the recipient, and is not acceptable from security professionals.

It is also made clear under the Human Rights Act that all people have the right to be free from discrimination.

The Human Rights Act is a worldwide charter.

Most of what it covers is also included in the Equality Act, Health & Safety at Work etc Act 1974 and other UK legislation.
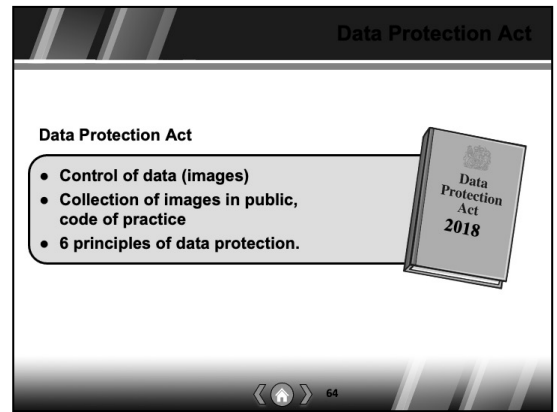
Main articles of interest are on the next slide.

Human Rights Act articles:

Article 2	right to life
Article 3	prohibition of torture
Article 5	right to liberty and security
Article 6	right to a fair trial
Article 7	no punishment without law
Article 14	prohibition on discrimination.

MY RIGHTS

There are more articles within this Charter.

Data Protection Act

- Control of data (images)
- Collection of images in public, code of practice
- 6 principles of data protection.

Data Protection Act 2018

64

The Data Protection Act 2018 enabled the General Data Protection Regulation (GDPR).

It can be anything from:

- a name
- a photo
- an email address
- bank details
- social media posts
- biometric data
- medical information.

It will also introduce 'digital rights' for individuals.

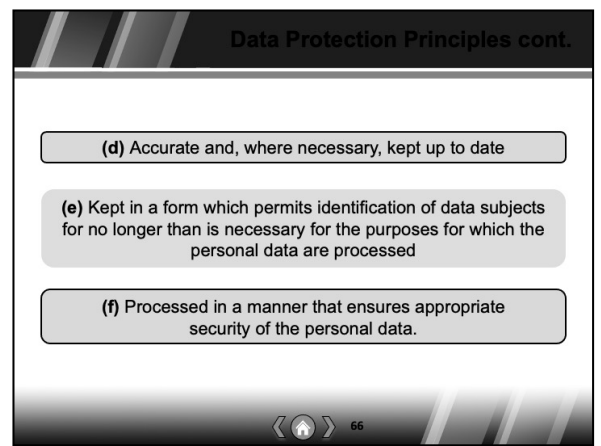**(a)** Processed lawfully, fairly and in a transparent manner

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

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

1 – as per operational requirement (ICO approval), e.g. health and safety and security for CCTV

2 – e.g. not for staff performance unless employees have agreed this use and is part of the operational requirement.

3 - e.g. information for employment records

(d) Accurate and, where necessary, kept up to date

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

(f) Processed in a manner that ensures appropriate security of the personal data.

4 - e.g. up-to-date addresses and phone numbers of all employees

5 – employment records, e.g. bank details, should not be kept once an employee that has left the business has been fully paid

6 – passwords etc.

Data protection rules often apply to the use of written records and notebooks, as well as the use of body-worn cameras.

You can find more information about the General Data Protection Regulation 2018 here:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protectionregulation-gdpr/?q=digital

Body-worn cameras (BWC)

- The wearer does not require a CCTV operator licence
- Must be clearly visible to the person(s) it is recording
- Images must be downloaded by an authorised person
- Images must be stored securely on an approved system
- Camera does not replace the need to complete your notebook or company documentation, e.g. incident reports.

67

- The owner (business) of the BWC must have approval with the ICO to use this equipment
- Individuals named on the CCTV-authorised list can download and review
- Storage system and length of storage is stated on the ICO approval

1 Describe civil law and criminal law.
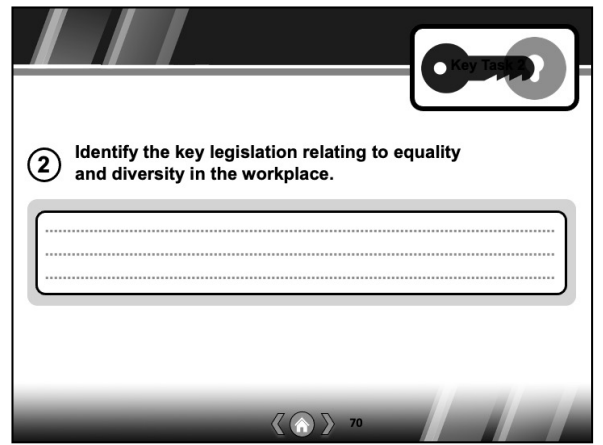
Civil law	Criminal law

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

Key Tasks

1 Describe civil law and criminal law.

Civil law	Criminal law
Civil law helps govern our daily lives	Criminal law prevents people from committing more serious offences, usually against people or property.

69

② **Identify the key legislation relating to equality and diversity in the workplace.**

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

② **Identify the key legislation relating to equality and diversity in the workplace.**

The Equality Act 2010.

3 Explain how the data protection regulation impacts your role as a security operative.

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

③ Explain how the data protection regulation impacts your role as a security operative.

The legislation covers any information related to a person or 'data subject' that can be used directly or indirectly to identify them e.g. incident reports, notebooks, identification, CCTV.

Arrest Procedures

Module 1:3

74

Completion of this module will enable learners to meet the following learning outcome:

Learning outcome 3: Understand arrest procedures relevant to security operatives

This includes assessment criteria:

3.1 State the meaning of arrest

3.2 Identify offences for which a security operative can make an arrest

3.3 Identify the limitations to a security operative's powers of arrest

3.4 State procedures to follow when making an arrest

3.5 State why an arrest should only be made as a last resort

3.6 State procedures following an arrest

3.7 State what is meant by 'reasonable' and 'necessary' force

This module includes the following interactive activities:

 Key task 3

An **arrest** or apprehension is
the taking or restraint of a person from his liberty
in order that he shall be forthcoming to answer an
alleged crime or offence.

It is a good idea to advise learners to learn their local arrest policies and work with their local police in relation to arrest.

Arrest is a last resort

Taking away someone's liberty is a very serious matter. Prior to acting, you must consider:

- whether you have powers of arrest (is it an indictable offence?)
- how long until/can the police attend?
- how you are going to stop the person from leaving and where are you going to this?
- whether you have a colleague to act as your witness
- if you are covered by CCTV
- if the person is likely to attempt to assault you

Remember, your safety is as important as a customer's safety.

Discuss what the police response time is for the area that you are teaching in.

Certain serious offences have been given a special condition within the criminal law and are known as 'indictable offences'

The majority of serious crimes that security operatives come across will fall within this category

Indictable offences are those that may be tried at a Crown Court.

In Scotland the term is arrestable, not indictable, offences.

Indictable offences are defined under Section 24a of the Police and Criminal Evidence Act 1984 (PACE) Article 26 PACE (Northern Ireland).

Section 24a of the Police and Criminal Evidence Act 1984 says that:

1) A person other than a constable (which includes security operatives) 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
2) Where an indictable offence has been committed, a person other than a constable may arrest without a warrant:
   a) Anyone who is guilty of the offence
   b) Anyone whom he has reasonable grounds for suspecting to be guilty of it.

78

Section 24a of the Police and Criminal Evidence Act 1984 (as amended by the Serious Organised Crime and Police Act of 2005). This Act was brought in to address the difficulties of the numerous and varied powers of arrest from the past, and now provides a power of arrest for most criminal offences where such a power is necessary (Article 26 PACE (Northern Ireland).

Constable means a warrant police officer.

A person other than a constable means non warranted individuals including security operatives hence the term Citizen's Arrest.

But this power of arrest is only exercisable if:

a) The person making the arrest has reasonable grounds for believing that for any of the reasons mentioned it is necessary to arrest the person in question

b) It appears to the person making the arrest that it is not reasonably practicable for a constable to make it instead

Security operatives have no more powers of arrest than any other citizen.

But this power of arrest is exercisable only if:

- the person making the arrest has reasonable grounds for believing that for any of the reasons mentioned it is necessary to arrest the person in question; and

- it appears to the person making the arrest that it is not reasonably practicable for a constable to make it instead.

The limitations to powers of arrest

Under Section 24a of the Police and Criminal Evidence Act (PACE) 1984, (the Criminal Procedure (**Scotland**) Act 1995, S26a of the Police and Criminal Evidence (Northern Ireland) Order 1989 (SI 1989/1341), certain serious offences have been given a special condition within criminal law and are known as indictable offences. The majority of crimes that security operatives come across will fall within this category. Indictable offences are those that may be tried at a Crown Court.

Offences under this section, for which all security operatives have the same powers of arrest as other members of the public include:

- murder/homicide
- culpable homicide
- assault (ABH, GBH and GBH w/i)
- rape
- sexual assault
- firearms offences
- drugs offences
- robbery
- theft
- burglary/housebreaking
- fraud
- criminal damage and malicious mischief (Scotland).

Offences under this section, for which all door supervisors have the same powers of arrest as other members of the public include:

- murder (also known as culpable homicide in Scotland)
- aggravated assault (also known as serious assault in Scotland) - legally known as GBH with intent
- burglary (also known as housebreaking in Scotland)
- criminal damage (also known as malicious mischief in Scotland)

A breach of the peace is a common law concept that has very ancient roots

In general terms it is considered to be:

'any disorder or disruption to the peace in public or in private that results in violence, threat of violence or provokes violence from another'.

Breach of the Peace

• A breach of the peace is a common law concept that has very ancient roots.

• In general terms it is considered to be *'any disorder or disruption to the peace in public or in private that results in violence, threat of violence or provokes violence from another'*.

This common law is not an indictable offence. Therefore the person cannot be charged with a breach of the peace. They may be charged under a different piece of legislation, e.g. Offence Against the Person 1861.

Citizen's arrest only refers to indictable offences, therefore a security operative would not be able to arrest for a breach of the peace.

Scotland

Breach of the peace in Scots law

Breach of the peace is a common law offence against society and is defined as 'conduct severe enough to cause alarm to ordinary people and threaten serious disturbance to the community'. The words 'severe' and 'serious' above are an essential element of breach of the peace and therefore it is not considered a trivial crime. Some breaches of the peace might be more 'minor', such as cursing or swearing in public, peering in a person's window or shop window and causing alarm to other people, or more serious incidents such as fighting in public or conducting oneself in a riotous or disorderly manner.

The common law crime of breach of the peace is that it can be committed by 1 or more people, so long as the conduct of the person or people is riotous or disorderly, while the conduct must be severe enough to cause alarm to ordinary people and threaten serious disturbance to the community *(Common law)*.

Security operatives should only arrest someone for one of the following reasons:

a) To prevent an offence being committed

b) To prevent the continuance of an offence

c) To prevent the renewal of an offence

d) To detain someone for an offence already committed.

The individual must be committing an indictable offence (arrestable in Scotland).

The person must be told:

Who you are (if not obvious); *'I am a member of the security team here'*	The grounds for the arrest; *'I have just seen you breaking that window'*
That they are under arrest; *'You are under arrest……..'*	That the police will be called. *'We are calling the police and you must wait here until they arrive'.*
What they are being arrested for; *'…….for criminal damage'*	

We are calling the police and you must wait here until they arrive.

84

Where possible, arrests should be made as quietly and as discreetly as possible to avoid situations from escalating and becoming out of control.

Security operatives should take care not to show an over-aggressive attitude when effecting an arrest, just a firmness of intent.

Once the decision has been made to arrest someone, the person must be told that they are under arrest as per the slide.

When carrying out an arrest:

- use everyday words
- do not 'caution' the suspect
- explain the reasons for the arrest
- only use force, if necessary, to prevent escape or assault
- treat the person reasonably
- you are in charge of their welfare until the police arrive.

Always consider how long the police may take to arrive at the scene. Do you really need to arrest the person or do you have sufficient evidence, e.g. good CCTV evidence, for the police to be able to arrest them at a later time?

Once you have arrested someone, you are responsible for their safety. You will need an area to keep them and CCTV, or at least 2 members of staff, to monitor them.

After an arrest, you are responsible for the person

You must:

- ensure own safety
- ensure the person's safety
- ensure the evidence is preserved
- hand over the person and the evidence to the police; explain reason for arrest in front of person and police
- record the arrest
- assist police with a statement
- possibly attend court to give evidence
- discuss the arrest procedure with the police.

86

After the arrest

Having arrested someone, you are then responsible for the suspect's welfare and safe custody until the arrival of the police.

You need to explain the reason for the arrest and how it was done to the police in front of the person as this is their opportunity to claim it was an unlawful arrest. If the person pleads guilty at court you will not need to attend the hearing.

While you have access to a police officer, you may wish to ask for some feedback on your arrest technique.

- You can use your powers of arrest in the course of crime prevention and detection
- Relatively few successful civil/criminal actions have been taken against security staff for unlawful arrest
- Use discretion and common sense when deciding when to effect an arrest
- Ensure you have the power to arrest in the first place.
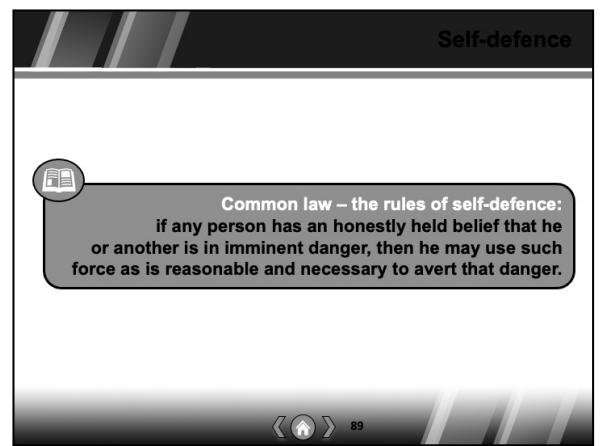
87

Unlawful/false arrest

Provided that discretion and common sense are used in deciding when to effect an arrest, and that when you are making the arrest you have reasonable grounds to suspect that the person is either committing or has committed an indictable offence, then you should not encounter too many problems.

Never put yourself in any unnecessary danger while effecting an arrest

If you are in any doubt about your ability to make the arrest, or about your personal safety, then the police should be called to:

- assist with the arrest
- make the arrest themselves.

Common law – the rules of self-defence:
if any person has an honestly held belief that he
or another is in imminent danger, then he may use such
force as is reasonable and necessary to avert that danger.

Scotland: 'In Scots law, if a person is attacked, or is in reasonable fear of attack, he's entitled deliberately to use such force as is needed to ward off that attack.'

If you feel that you are about to be attacked, you don't need to wait for someone else to strike the first blow. Circumstances may justify a pre-emptive strike.

So, if a door supervisor (while on duty) feels that they or someone else is about to be hurt, then they are allowed to use force to protect themselves or that other person.

In a criminal case in 1988, it was said that common law has always recognised the right of a person to protect themselves from attack and to act in the defence of others, and if necessary, to inflict violence on another in so doing. Provided that no more force is used than is reasonable to repel the attack, such force is not unlawful and no crime is committed.

In another case in 1995, it was said that the necessity of using force was a question for the subjectivity of the defendant, whereas the degree of force was more objectively considered by the courts. This means that door supervisors have to decide themselves if and when to use force, whereas ultimately a court may have to decide whether the amount of force used was reasonable or not.

Security operatives do occasionally need to use force to carry out their duties and, under certain circumstances, are legally empowered to do so. Force can be used if:

- being used for self-defence
- saving life/saving others from harm
- preventing someone from leaving after an arrest (citizen's arrest).

90

The use of force

The law gives certain situations when members of the public are allowed to use force on others, and the authority for door supervisors to use force when necessary can be found in the following parts of the law:

- self-defence
- breach of the peace/saving life
- Sec.3 Criminal Law Act.

Sec.3 Criminal Law Act, 1967

This act gives everyone, including door supervisors, the authority to use:

'such force as is reasonable in the circumstances in the prevention of crime, or in effecting (or assisting in) the lawful arrest of offenders, suspected offenders or persons unlawfully at large'.

'Prevention of crime' applies to any crime where the preventative use of force is reasonably required, including protecting property from damage/theft and protecting people from physical injury.

The Criminal Law Act allows door supervisors to use force to stop a crime from being committed or to arrest someone and stop them from running away before the arrival of police.

It is important to remember that the wording of this act refers to *'such force as is reasonable in the circumstances'*, and previous criminal cases have pointed out that where force is used in these situations, the amount of force used must be judged according to the particular circumstances. It is made very clear, however, that the excessive use of force is not allowed.

If security operative considers that every time they use force against another person that they may well have to justify their actions, then they should be able to act reasonably in any given situation. If, however, they are reckless as to how much force they use, or deliberately use excessive force, then they will have to answer to the police and possibly even to a court.

Was the force used necessary?

This is a matter of opinion. Questions that are likely to be asked about any use of force are:

1. Was there a need to use the force?
2. Was the amount of force used reasonable?
3. What was the extent of the injuries compared to the amount of resistance given?
4. What was the size and build of the injured party compared to the door supervisor?
5. Were any weapons used or threatened by the other party?
6. At what stage did the security operative stop using the force?
7. Was the force applied in good faith or in a malicious way?

92

The questions that are likely to be asked about any use of force are:

(1) Was there a need to use the force? Were they leaving anyway?

(2) Was the amount of force used reasonable or not? What did they do and what did we do?

(3) What was the extent of the injuries compared to the amount of resistance given? If they did not struggle, why/how did we damage them?

(4) What was the size and build of the injured party compared to the door supervisor? This is not about big security officer versus small skinny person, it is about whether we used the minimum amount of force possible or if we approached with full force and power.

(5) Were any weapons used or threatened by the other party? If yes, you do what you have to do with what you have access to.

(6) At what stage did the security operative stop using the force? Once they are outside the premise/shop, why do we still have a hold on them?

(7) Was the force applied in good faith or in a malicious way? Is there any personal connection as to why you might want to hurt this person? If yes, ideally, it should not be you applying any force.

Hand on heart, everyone knows whether the force was genuinely reasonable and necessary or whether 'red mist' (anger) was a part of our actions.

1 Explain what is meant by the term 'arrest'.

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

1 **Explain what is meant by the term 'arrest'.**

The taking or restraint of a person from their liberty in order that they
shall be forthcoming to answer an alleged crime or offence.

2 Provide SIX examples of offences for which a security operative can make an arrest.

1 ....

2 ....

3 ....

4 ....

5 ....

6 ....

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

2 Provide SIX examples of offences for which a security operative can make an arrest.

1 Murder

2 Rape

3 Assault (ABH, GBH and GBH w/i)

4 Sexual assault

5 Drug offence

6 Robbery.

3 Explain the procedures a security operative should follow after an arrest.

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

3 **Explain the procedures a security operative should follow after an arrest.**

You are responsible for the suspect's welfare and safe custody until

the arrival of the police.

Health and safety

Module 1:4

Completion of this module will enable learners to meet the following learning outcome:

Learning outcome 4: Understand the importance of safe working practices

This includes assessment criteria:

4.1 Identify responsibilities under the Health and Safety at Work etc. Act

4.2 Identify the risks of lone working within the private security industry

4.3 Identify typical workplace hazards and risks

4.4 State how to minimise risk to personal safety at work

4.5 Identify safety signs and signals

4.6 State procedures to be followed for recording and reporting accidents and health and safety incidents

4.7 Identify ways to keep personal information safe

This module includes the following interactive activities:

- class question: What are the employer's responsibilities?
- class question: What are the employee's responsibilities?
- class question: What items of personal protective equipment (PPE) might a security operative carry?

Key task 4

Health and safety in the workplace

Every year, thousands of people have time off work due to sustaining injuries that could have been avoided

KEY POINT
Health and safety procedures are there to keep everyone safe.

101

Health and safety in the workplace

Every year, thousands of people in the UK are forced to take time off work due to health and safety-related issues. For some, this may only mean a few days off work but for others, it could mean long-term injuries or even death.

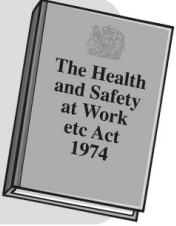The vast majority of incidents can be avoided through better health and safety procedures.

Health and safety procedures in our places of work need to be effective to keep staff, visitors and customers safe.

There is specific legislation in place to ensure that proper health and safety procedures are enforced anywhere that people work or come to be served.

Covers:

- employers
- employers
- the self-employed
- subcontractors
- Suppliers
- people who control premises
- visitors/customers on the site.

The Health and Safety at Work etc. Act 1974 (Health and Safety at Work (Northern Ireland) Order 1978) covers employers, employees, the self-employed, suppliers, people who control premises and visitors/customers who come onto the site.

Those failing to comply with health and safety legislation face a range of penalties, and businesses can be closed for serious breaches.

Breaches

Breaches of the legislation can be dealt with by either:

● The Health and Safety Executive (HSE)
● The local environmental health practitioner (EHP) from the local authority

Breaches can result in:

● improvement notices
● prohibition notices
● criminal proceedings.

103

As well as the above examples, the next slide details other negative consequences that can come from breaching health and safety legislation.

Other negative consequences of breaches:

loss of productivity

business disruption

staff shortages

possible long-term effects
on employees.

Further to legal implications, companies and organisations that have poor health and safety policies and procedures can suffer from the above negative consequences.

Duty of care:
A moral or legal obligation to ensure the health, safety and welfare of others.
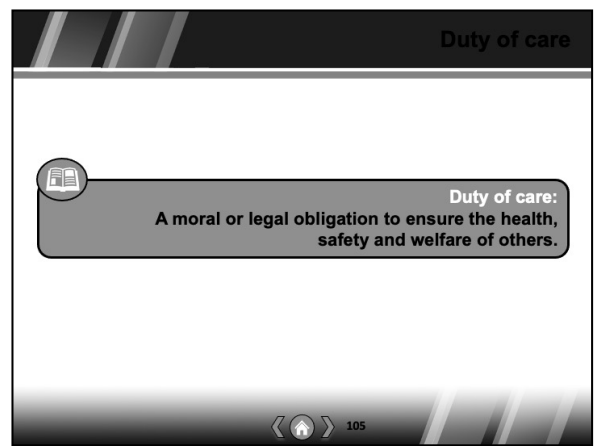
Employers have a moral and legal duty of care to protect the health, safety and welfare of their employees and others, including customers and members of the public who might be affected by their business. Employers must do whatever is reasonably practicable to achieve this.

Serious breaches of health and safety legislation can result in penalties of up to 2 years' imprisonment and/or unlimited fines.

Employers must:

- carry out a risk assessment
- do what they can to remove or reduce risks
- provide safety equipment
- ensure safe working procedures
- provide relevant instruction and training
- provide suitable personal protective clothing or equipment (PPE).

106

Class question: What are the employer's responsibilities?

Safety equipment can include relevant warning signs.

Employers must also provide proper first-aid facilities, ensuring that there are proper reporting procedures in place in case of incidents.

Depending on the size of the site and the number of people working there, they may have to also provide a written health and safety policy.

Class question: What are the employee's responsibilities?

The above is true regardless of whether employees/the self-employed are full or part-time staff.

In ensuring that they do not act in an unsafe manner, employees must ensure that not only are they caring for their own health and safety, but also that they are not putting the health and safety of others at risk.

If serious incidents occur they must follow the site or organisation's emergency procedures to help protect themselves, other staff and any visitors/customers.

They must then follow the site's reporting procedures to inform the employer of any accidents and/or injuries.

Hazard:
something with the potential to cause harm

Risk:
the likelihood of harm occurring

Risk assessment:
the identification of hazards, the calculation of risk and the reduction of that risk, either completely or to an acceptable level

Good health and safety practices are all about reducing hazards and risks.

108

Hazard: potential source of harm or adverse health effect on a person.

Risk: likelihood that a person may be harmed or suffer adverse health effects if exposed to a hazard. Levels of risk may be, high, medium or low impact.

Risk assessment: the identification of hazards, the calculation of risk and the reduction of that risk, either completely or to an acceptable level.

Good health and safety practices are all about reducing hazards and risks.

Typical risks and hazards in the workplace include:

- slips, trips and falls
- injuries from poor manual handling
- misuse/abuse of machinery
- sharp objects like needles and knives
- diseases
- hazardous chemicals
- global or critical incidents
- noise pollution
- moving vehicles
- locked or blocked fire exits
- obstructions
- poor lighting
- overcrowding
- fires, floods and other emergencies
- unsuitable footwear.

Typical risks and hazards in the workplace also include:

- accidents due to poor lighting, uneven surfaces, steps, etc.

- infection from body fluids

- dealing with aggressive behaviour

- spillages, e.g. cleaning chemicals

Ask the learners to give examples of risks and hazards they will come across in their workplace as a security operative.

In relation to global (or critical) incidents such as pandemics, epidemics, acts of terrorism, etc. you must ensure that you follow all relevant health and safety policies and organisational procedures. In the case of a pandemic, you may find that you are required to work from home where possible, if this is not possible then you may be asked to wear additional PPE such as face masks when in the workplace. You can find further information on the .gov website and the World Health Organisation website https://www.who.int/ about current global incidents.

Once a hazard or risk has been identified, follow the hierarchy of control to work out the best ways to deal with the potential problem.

110

**Minimising risks to personal safety and security**

Ask the questions:

- can the hazard be eliminated?
- can the hazard be substituted with a reduced risk?
- can the hazard be isolated or enclosed?
- would the introduction of a safe system of work reduce the risk? For example, new procedures and routines.
- would information, training or supervision reduce the risk?
- would PPE help?

There are 5 steps to carrying out a risk assessment:

Step **1** Identify the hazards

Step **2** Identify who may be harmed and how

Step **3** Evaluate the risk and introduce further controls

Step **4** Record the findings and implement them

Step **5** Review and revise and update if necessary.
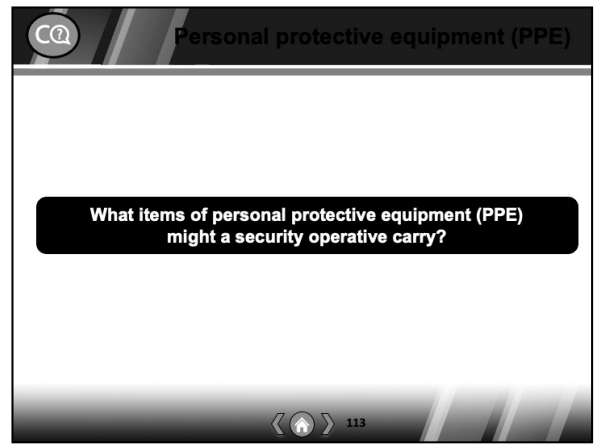
What items of personal protective equipment (PPE) might a security operative carry?

Class question: What items of personal protective equipment (PPE) might a security operative carry?

Click to reveal the answer.

Security operatives will carry the following PPE:

- waterproof clothing
- high-visibility clothing
- headwear
- gloves (needle/slash resistant)
- rubber gloves and face-shields
- stab-resistant vests
- ear defenders
- eye protection
- safety footwear
- face masks/coverings (infectious diseases)

Equipment:
- metal detectors and/or mirrors
- body cameras
- radios
- mobile phones
- personal alarms
- torches
- equipment as it applies to the incident e.g. to help control infection.

114

Security operatives will carry needle/slash-resistant and rubber gloves to protect themselves from both physical injury and body fluids.

Face-shields are worn also to protect against body fluids.

Metal detectors and/or mirrors are used for searching.

Safe manual handling

Manual handling is the movement or support of any load by physical effort, including lifting, moving, carrying, pushing and pulling

If you lift or move heavy objects without using the recognised procedures, you run the risk of sustaining the following injuries:

- fractures
- spinal disc injuries
- trapped nerves
- friction burns
- damage to muscles
- damaged ligaments and tendons
- abrasions and cuts
- hernias.

It is important that safe routines are followed to avoid the risk of the above injuries. The following slides will introduce LITE, procedures to follow when lifting a load.

Before attempting to lift a load, use LITE to evaluate the risk:

L I T E

L

LOAD

Look at the load. If it is too heavy, can it be lightened or split? If it is unstable, can handles be fitted or the load be reapportioned?

I

INDIVIDUAL

Consider the capability of the person. Are they strong or fit enough? Are they adequately trained for the task?

T

TASK

Evaluate the job to be done. Does the task involve stretching, twisting or bending? Can machinery be used or can team handling be used?
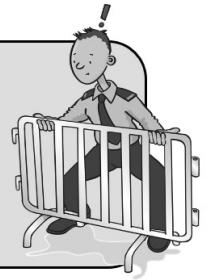
E

ENVIRONMENT

Control the environment where the task takes place. Is the floor slippery or uneven? Can the layout or floor condition be improved?

The 6 safe lifting techniques are:

1. Stop and think
2. Position the feet
3. Bend the knees
4. Get a firm grip, keeping the back slightly flexed
5. Raise with the legs
6. Raise with the legs
7. Keep the load close to the body.

Security operatives who work alone can be particularly susceptible to:

- violence
- injury
- ill health
- lack of support/communication
- lack of welfare facilities for rest.

Security operatives who work alone can be at high-risk in the workplace.

They may feel isolated if they only have technological means with which to communicate with colleagues or call for assistance.

Technology can often fail to work in the manner it was intended.

Safety signs and signals

Safety signs and signals:

- are used to communicate health and safety instructions
- must be kept clean
- must be displayed where they can be easily seen.

120

Security operatives must be aware of the colour, shape and purpose of each category of safety sign/signal.

Prohibition signs mean that you are prohibited from doing something.

No mobile phones

121

Prohibition signs mean that you are prohibited from doing something.

Mandatory signs mean that you must do something.

Fire door
Keep shut

Keep
out

BLUE

122

Mandatory signs mean that you must do something.

Safe condition signs indicate where to go for safety.

First aid box

GREEN

123

Safe condition signs indicate where to go to for safety.

Warning signs indicate a specific danger.

YELLOW

CAUTION
Slippery floor
surface

DANGER
High Voltage

124

Warning signs indicate a specific danger.

Fire safety signs indicate firefighting equipment.

Fire extinguisher

For fire use only

RED

125

Fire safety signs indicate fire fighting equipment.

**Hazardous substances signs warn
you about dangerous chemicals.**

126

Hazardous substances signs warn you about dangerous chemicals.

Incidents and accidents must be properly reported to:

- meet legal requirements
- help identify accident trends
- improve practices and procedures
- help prevent similar incidents
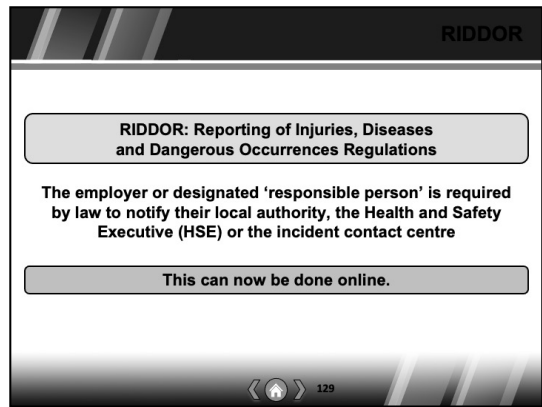- assist with insurance claims and investigations.

Following any accident or medical incident, it is important to record all of the details relating to the situation. The information contained in the accident or incident book can help employers to identify accident trends, so they can then improve practices and procedures on the site to prevent similar incidents.

These records may also be required for insurance and/or investigative purposes.

Information required

Incident/accident reports need to include at least the following information:

- day, date and time of incident
- location of incident
- how you were alerted to it
- what you saw
- what you were told
- what happened
- what action you took
- whether first aid was required
- whether the emergency services were called
- what the result was
- details of any injuries
- details of any witnesses
- any descriptions of property or people.

128

Reports need to be made as soon as possible after the incident/accident has finished, while events are still fresh in the mind.

RIDDOR: Reporting of Injuries, Diseases and Dangerous Occurrences Regulations

The employer or designated 'responsible person' is required by law to notify their local authority, the Health and Safety Executive (HSE) or the incident contact centre

This can now be done online.

129

Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR)

For serious accidents, incidents and near misses at work, the employer or the designated 'responsible person' is required by law to notify their local authority, the Health and Safety Executive (HSE) or the incident contact centre. This can now be done online.

The Data Protection Act 2018 (GDPR), covers any information related to a person or 'data subject' that can be used to directly or indirectly identify them

It can be:

- anything from a name, a photo and an email
- address to bank details, social media posts,
- biometric data and medical information.

The Data Protection Act 1998

130

The Data Protection Act/GDPR, covers any information related to a person or 'data subject' that can be used to directly or indirectly identify them. It can be anything from a name, a photo and an email address to bank details, social media posts, biometric data and medical information.

The Data Protection Act will be covered in more detail later in the course.

Personal information can be kept safe by:

- following all organisational procedures
- following assignment instructions
- maintaining confidentiality of information
- using social media in a responsible way; this includes having the highest levels of security settings on your accounts

- not wearing anything identifiable outside the workplace
- demonstrating personal vigilance, e.g. not completing surveys
- not discussing work issues outside the workplace
- not discussing work information with colleagues.

Key Task 1

① **Identify the responsibilities of employees and employers under the Health and Safety at Work Act.**

Employees	Employers

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

1 **Identify the responsibilities of employees and employers under the Health and Safety at Work Act.**

Employees	Employers
Employees must follow the site's health and safety policy at all times	Employers must carry out a proper risk assessment of any possible risks to employees and other people visiting the site. They must do what they reasonably can to either remove or reduce those risks.

2 **Identify FOUR risks associated with lone working.**

1 ....

2 ....

3 ....

4 ....

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

2 Identify FOUR risks associated with lone working.

1	Violence
2	injury
3	Ill health
4	Lack of communication.

(3) State the procedures that should be followed for recording and reporting accidents and health and safety incidents.

Accidents	Health and safety incidents

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

3 State the procedures that should be followed for recording and reporting accidents and health and safety incidents.

Accidents	Health and safety incidents
record all information in the accident book	record all information in the incident book.
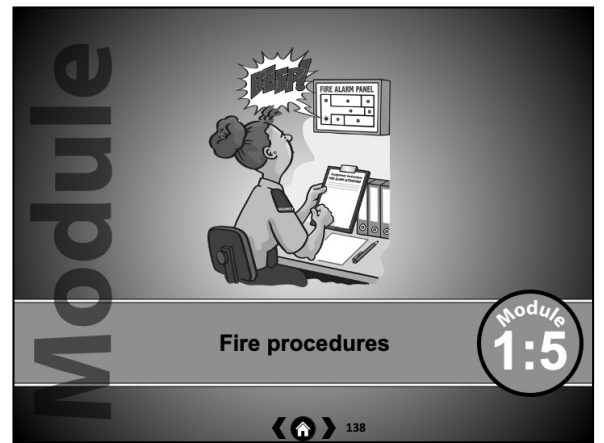
Fire procedures

Module 1:5

Completion of this module will enable learners to meet the following learning outcome:

Learning outcome 5: Understand fire procedures in the workplace

This includes assessment criteria:

5.1 Identify the elements that must be present for fire to exist

5.2 State the actions to be taken upon discovering a fire

5.3 Identify basic fire safety controls

5.4 Identify classifications of fire

5.5 Identify the different types of fire-fighting equipment

5.6 Identify the role of a fire marshal in the event of an emergency

This module includes the following interactive activities:

Key task 5

Fire safety measures

Fire safety on the premises or the site is important for both staff and any visitors or customers.

If a fire occurs in the workplace, it could result in the disruption of the normal business activities and affect profitability.

More importantly, staff and/or customers could be injured or even lose their lives.

Good fire safety is, therefore, everyone's responsibility.

Basic fire prevention measures include:

- switching off all non-essential electrical appliances
- not overloading electrical points
- regularly inspecting and maintaining all electrical equipment
- safely storing flammables
- regularly emptying ashtrays
- storing rubbish away from the building
- keeping electric and gas fires well away from furniture.

140

Basic fire prevention measures can be extremely useful in helping to prevent the chances of a fire starting to begin with.

To help prevent the chances of a fire starting, everyone should be mindful of the following:

- all non-essential electrical appliances should be switched off

- electrical points should not be overloaded

- all electrical equipment should be inspected regularly and maintained properly

- flammables must be stored safely

- ashtrays should be emptied regularly

- rubbish should be stored away from the building

- electric and gas fires must be kept well away from furniture

Under the Regulatory Reform (Fire Safety) Order of 2005 (Fire (Scotland) Act 2005), employers must:

- nominate a competent person to carry out a full fire risk assessment
- provide their employees with any relevant information, instruction and training

Security operatives must also cooperate with their employers in all matters relating to fire safety.

141

Under the Regulatory Reform (Fire Safety) Order of 2005, (Fire (Scotland) Act 2005) employers must nominate a competent person to carry out a full fire risk assessment for the site, which **must** be documented.

They must also provide their employees with any relevant information, instruction and training to ensure their safety while working on the site.

Employees such as security operatives must take responsibility for their own health and safety, and for that of others. They must be observant, vigilant and also cooperate with their employers in all matters relating to fire safety. This includes following any training and adhering to the fire plan.

Fire needs 3 elements to start and survive. They are heat, fuel and oxygen.

3

Oxygen
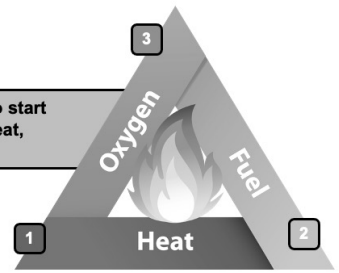
Fuel

1 Heat 2

If any of these 3 elements are greatly reduced or removed, then the fire itself will be reduced or extinguished

1. **HEAT** - a minimum temperature is needed to start a fire and for it to continue
2. **FUEL** - fire needs something to burn, like solid fuel, oil or gas
3. **OXYGEN** - fire needs oxygen to burn, as it supports the combustion process.

If any of these three elements are greatly reduced or removed, then the fire itself will be reduced or extinguished.
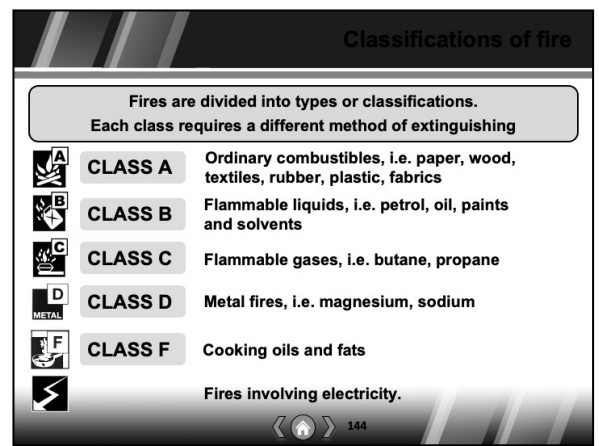
- **HEAT** - a minimum temperature is needed to start a fire and for it to continue.

- **FUEL** - fire needs something to burn, like solid fuel, oil or gas.

- **OXYGEN** - fire needs oxygen to burn, as it supports the combustion process.

Fires are divided into types or classifications.
Each class requires a different method of extinguishing

	CLASS A	Ordinary combustibles, i.e. paper, wood, textiles, rubber, plastic, fabrics
	CLASS B	Flammable liquids, i.e. petrol, oil, paints and solvents
	CLASS C	Flammable gases, i.e. butane, propane
	CLASS D	Metal fires, i.e. magnesium, sodium
	CLASS F	Cooking oils and fats
		Fires involving electricity.

144

Fires are divided into types or classes. Each class requires a different method of extinguishing and so it is important that we understand the differences.

- **CLASS A** – Paper, wood, textiles, rubber, plastic, fabrics
- **CLASS B** – Flammable liquids, i.e. petrol, oil, paints and solvents
- **CLASS C** - Flammable gases, i.e. butane, propane
- **CLASS D** - Metal fires, i.e. magnesium, sodium
- **CLASS F** - Cooking oils and fats

No class for fires involving electricity.

Fire extinguishers:

- are used for small fires
- have a limited capacity
- can be easily carried to a fire
- intended for use by anyone

Security operatives need to know their:

- uses
- locations
- methods of operation.

WATER

145

Fire extinguishers:

- are generally used to fight small fires, in an effort to prevent them spreading and causing large-scale damage

- have a limited capacity, but they can be easily carried to the fire and quickly put to work

- are intended to be used by anyone who needs them, so it is important that all members of staff learn of their uses, locations and methods of operation

- should be sited in conspicuous locations on escape routes, such as next to exits and in corridors and should be mounted on wall brackets

Different types of extinguishers are designed to fight different classes of fire, so it can be useless or even dangerous to use the wrong type of extinguisher at the scene of a fire.

Fire extinguishers cont.

Fire classification	Fire risk	Water	Foam	CO₂	Powder	Wet Chemical
Class A	Paper, wood, textiles and fabrics	✓	✓		✓	✓
Class B	Flammable liquids: petrol, oil, paints and solvents		✓	✓	✓	
Class C	Flammable gases				✓	
Class D	Metal fires such as magnesium and sodium				✓	
Class F	Cooking oils and fats					✓
	Electrical			✓	✓	

146

- Explain chart.

Contents gauge

Type of extinguisher

Method of operation

Class of fire suitable for use

Service maintenance date*

WATER
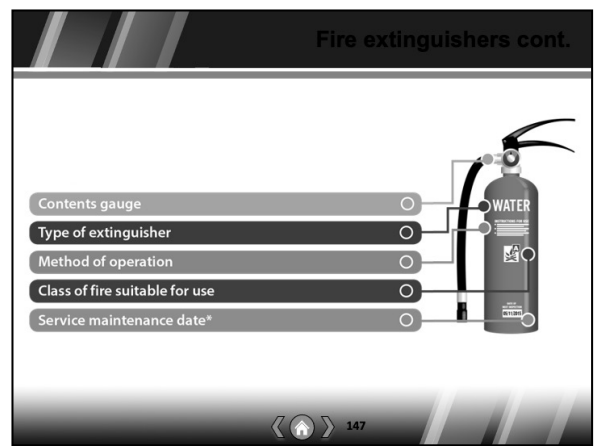
Explain chart.

All extinguishers should be inspected annually by a competent person, e.g. an extinguisher engineer.

Only attempt to fight the fire if:

- the alarm has been raised
- the emergency services have been contacted
- the fire is not spreading and is confined
- you have a clear escape route not threatened by fire
- you have selected the correct extinguisher.
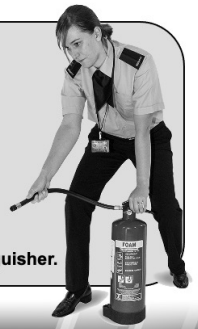
Do not attempt to fight a fire if:

- **it is bigger than a wastepaper bin (rule of thumb)**
- **you need more than 1 extinguisher**
- **the room is filling with smoke**
- **you do not have a clear escape route**
- **gas cylinders or chemicals are involved**
- **your efforts are not reducing the size of the fire**
- **you do not have the correct extinguisher.**

Operating an extinguisher

- Select the correct extinguisher
- Check contents gauge
- Pull the pin to break the seal
- Holding the extinguisher upright, squeeze the trigger
- Test the range and content (away from the fire)
- Extinguish the fire using the correct technique for that type of extinguisher and the nature of the fire.

It is important that all security operatives take the correct actions on discovering a fire

You will need to:

- follow the organisation's policies and procedures
- sound the alarm and inform emergency services
- follow the acronym of FIRE:
  - **Find** – you discover a fire
  - **Inform** – raise the fire alarm
  - **Restrict** – restrict access to the area of the fire
  - **Evacuate** – evacuate the building or extinguish (extinguish the fire if safe to do so).
- control panel: Important to ensure full understanding of the extent of the area of the incident, to pass on correct message to emergency services e.g. with regard to materials or chemicals stored in the affected area.

Most commercial and business buildings now have their own fire alarm systems

These are designed to detect fires as soon as they start, raise the alarm and sometimes to call the fire brigade automatically

Security operatives need to be aware of how their fire alarm system works and what they need to do on hearing the alarm.

152
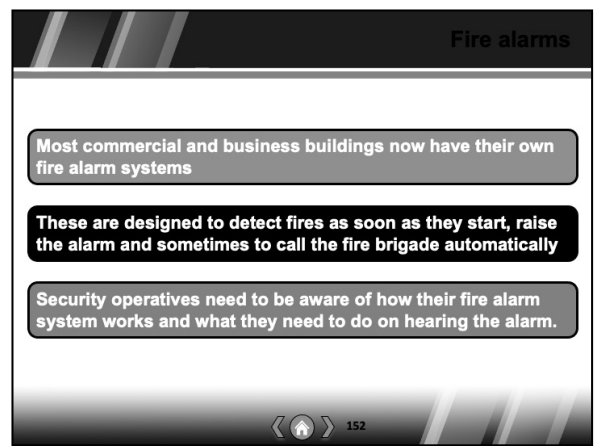
Fire alarms

Most commercial and business buildings now have their own fire alarm systems. These are designed to detect fires as soon as they start, raise the alarm and sometimes to call the fire brigade automatically.

Security operatives need to be aware of how their fire alarm system works and what they need to do themselves on hearing the alarm.

Fire blankets can be used to extinguish fires by smothering them. They are often found in kitchens, as they are very useful for extinguishing fat fires in pans.

FIRE BLANKET

Pull to release

Fire blanket

153

Fire blankets

Fire blankets can be used to extinguish fires by smothering them. They are often found in kitchens, as they are very useful for extinguishing fat fires in pans.

Some fire alarm systems are connected to sprinklers which spray water onto the fire from outlets in the ceiling, holding back the fire until the arrival of the fire service.

Long lengths of rubber hose positioned strategically around the site

Permanently connected to the mains water supply and are started by opening a valve before use

Can be quite heavy to unreel when needed, but are very effective when used as they provide a limitless supply of water.

155
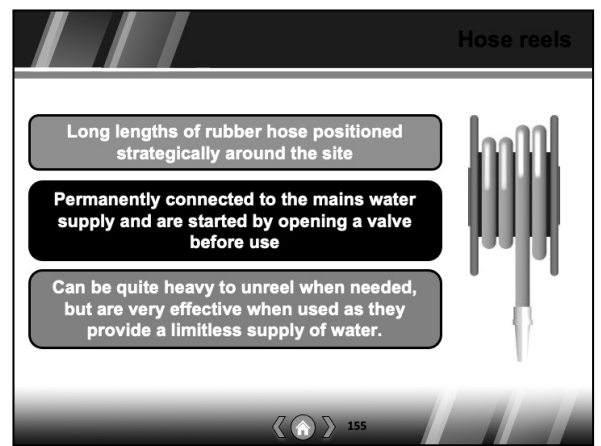
Hose reels

Hose reels are long lengths of rubber hose on large drums positioned strategically around the site.

The hoses are permanently connected to the mains water supply and are started by opening a valve before use.

They can be quite heavy to unreel when needed, but are very effective when used as they provide a limitless supply of water.

Some buildings have riser systems built in

These systems consist of long water pipes running along the outside of the building and across the ceilings on each floor, allowing water to be dispensed via sprinklers to each floor in the event of a fire
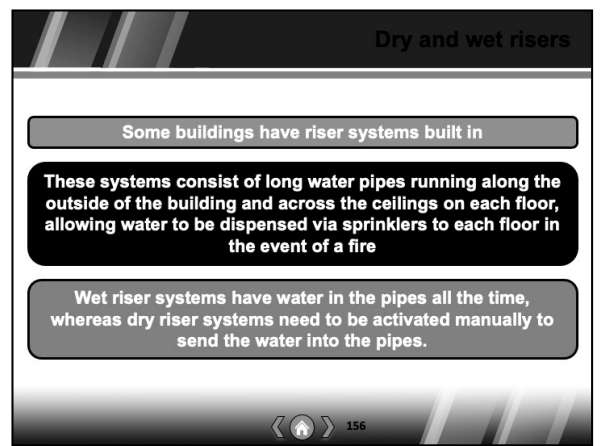
Wet riser systems have water in the pipes all the time, whereas dry riser systems need to be activated manually to send the water into the pipes.

Dry and wet risers

Some buildings, particularly multi-storey ones, have riser systems built in.

These systems consist of long water pipes running along the outside of the building and across the ceilings on each floor, allowing water to be dispensed via sprinklers to each floor in the event of a fire.

Wet riser systems have water in the pipes all the time, whereas dry riser systems need to be activated manually to send the water into the pipes.

- Flooding systems are designed to be used in unoccupied rooms where there are high-value contents or areas where a fire may cause major disruption to the activities of the organisation
- Examples might be archives, electrical equipment or switchgear
- On detection of the fire, a fire extinguishing medium (most commonly CO_2) will be discharged into the room to replace the air and extinguish the fire by smothering.

157

Flooding systems

Flooding systems are designed to be used in unoccupied rooms where there are high value contents or areas where a fire may cause major disruption to the activities of the organisation. Examples might be archives, electrical equipment or switchgear. On detection of the fire, a fire extinguishing medium (most commonly CO_2) will be discharged into the room to replace the air and extinguish the fire by smothering.

Internal fire doors:

- help prevent/reduce the spread of smoke and flames from one room to another
- should be closed at all times
- should not be obstructed

Fire exits:

- are vital as a means of escape in the event of a fire
- should be clearly marked
- must be unlocked when anyone is in the building
- should not be obstructed on the inside/outside.

158

Internal fire doors are used to help prevent or reduce the spread of smoke and flames from one room to another.

They should be closed at all times, **unless they can be closed electronically** if the fire alarm activates.

They should not be obstructed.

Fire exits are vital as a means of escape in the event of a fire.

They should be clearly marked, must be unlocked when anyone is in the building and should not be obstructed on the inside or the outside.

- The warning and controlling units within a fire alarm system
- If a fire emergency is detected, the control panel alerts those monitoring it via various lights and audible alarms
- Security operatives can work out the type of emergency, exactly where it is occurring and over what extent of an area
- Some systems actually call the fire brigade, sound the fire alarm, unlock doors, cut off electricity and set off sprinkler systems automatically.

Fire alarm control panels

These are the warning and controlling units within a fire alarm system.

Once a possible fire emergency is detected within the building or somewhere on the site, usually as the result of a signal from a smoke or heat detector, the control panel alerts those monitoring it via various lights and audible alarms.

By understanding the layout of the control panel, security operatives can work out what type of an emergency it is, exactly where it is occurring and over what extent of an area.

A decision can then be made as to what appropriate action to take, be it to inform a supervisor and then search the area concerned, to call the fire brigade immediately with information to tell them about the incident itself and any secondary dangers there might be.

Some of the more sophisticated systems actually call the fire brigade, sound the fire alarm, unlock doors, cut off electricity and set off sprinkler systems automatically.

If security operatives are required to monitor a fire alarm control system as a part of their duties, they need to properly understand how it works and what actions they personally need to take in an emergency.

In an evacuation, security operatives must:

- take control
- communicate effectively
- help to evacuate the site quickly and safely
- encourage people to leave via the safest exit
- assist anyone who does not know where to go
- assist any vulnerable people (elderly, disabled and children)
- avoid causing unnecessary panic
- know where the assembly points are
- know what to do once the building is empty.

160

Fire evacuation procedures

One of the most important roles for security operatives in the event of a fire will be ensuring that the site is evacuated quickly and safely.

Hopefully, both staff and visitors/customers that they should leave the building when they hear the fire alarm sounding. Security operatives must be available to encourage people to leave via the safest exit, and to assist anyone who does not seem to know what to do. Particular care needs to be taken to look after any vulnerable people like children, the elderly or those with physical or mental difficulties.

It is also important to try to avoid causing unnecessary panic. Security operatives need to take control of fire incidents in an assertive but calm manner. They need to show decisiveness, leadership and use clear, effective communication skills so that others understand how serious the situation is.

Security operatives also need to know where the fire assembly points are and what needs to be done once the building or site has been evacuated.

Typical actions would include:

- raise the alarm – yell 'fire' to warn others

- operate the nearest manual call point (if fitted)

- call the fire service (999)

- evacuate the area

- restrict access and isolate the fire

- report to the assembly point

- only attempt to fight the fire if it is safe to do so and you have been trained

Evacuation procedures need to be practised

Remember the 5 Ps:

P PLANNING and   P PREPARATION

P PREVENTS   P POOR   P PERFORMANCE

By acting promptly and correctly in times of emergency, security operatives can help to save time in the evacuation, keep themselves and others safe, assist the emergency services, prevent injuries and save lives.

162

Evacuation procedures need to be practised.

Remember the five Ps:

• P - Planning and

• P - Preparation

• P - Prevents

• P - Poor

• P - Performance

If security operatives act promptly and correctly in times of emergency, they can help save time in the evacuation, keep themselves and others safe, assist the emergency services, prevent injuries and save lives.

Fire wardens (sometimes called fire marshals) are members of staff who are nominated to take responsibility for a particular area with regards to fire safety. The numbers of nominated wardens/marshals will vary depending on the size of the site and the numbers of people involved.

Under the Regulatory Reform (Fire Safety) Order of 2005, (Fire (Scotland) Act 2005) they are there to assist the designated person responsible for fire safety generally.

The following list, although not exhaustive, details some of the specific duties usually given to fire wardens/marshals:

- assisting with fire risk assessments

- checking that all exit doors and escape routes are unlocked and unobstructed

- ensuring that all fire extinguishers are in the correct position with seals in place

- checking that all safety signs are clearly visible and in the correct place

List continues on following slide.

Typical duties include:

- making sure that all alarm call points are unobstructed and working correctly
- checking all fire doors are closed and functioning properly
- ensuring corridors and walkways are kept clear
- ensuring assembly points are clearly marked and easily accessible
- reporting any equipment faults.

165

The following list, although not exhaustive, details some of the specific duties usually given to fire wardens/marshals:

- making sure that all alarm call points are unobstructed and working correctly;

- checking that all fire doors are closed and functioning properly;

- ensuring that corridors and walkways are kept clear;

- ensuring that assembly points are clearly marked and easily accessible; and

- reporting any equipment faults

During a fire situation, their duties will include:

- sounding the alarm/calling the fire service
- assisting with the evacuation (strangers and vulnerable people)
- fighting the fire if it is safe to do so
- ensuring everyone is out of the building
- closing doors and windows
- manning the assembly point;
- taking or assisting with the roll call
- assisting the fire coordinator
- liaising with the fire service

Key Tasks

1. State the THREE elements needed for a fire to start and survive.

1. ....
2. ....
3. ....

167

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

1 **State the THREE elements needed for a fire to start and survive.**

1 Heat

2 Fuel

3 Oxygen.

② List FOUR tasks a fire warden/ marshal may be required to carry out.

1 ....

2 ....

3 ....

4 ....

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

2 List FOUR tasks a fire warden/marshal may be required to carry out.

1 Sounding the alarm

2 Checking allocated areas to ensure everyone has left

3 Taking control of the evacuation and ensuring anyone with evacuation difficulties is aided

4 Proceeding to the assembly area and reporting to the fire officer in charge.

Key Tasks

3 List FOUR classes of fire and their meaning.

1 ....
2 ....
3 ....
4 ....

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

3 List FOUR classes of fire and their meaning.

1 Class A – paper, wood, textiles, rubber, plastic, fabrics

2 Class B – flammable liquids i.e. petrol, oil, paints and solvents

3 Class C – flammable e gases i.e. butane, propane

4 Class D – metal fires i.e. magnesium, sodium

Class F – cooking oils and fats.

Module

Emergencies

Module
1:6

173

Completion of this module will enable learners to meet the following learning outcome:

Learning outcome 6: Understand emergencies and the importance of emergency procedures

This includes assessment criteria:

6.1 Identify the key emergency terms

6.2 Identify different types of emergencies within the workplace

6.3 Recognise how people react when emergencies occur

6.4 Identify actions to be taken in an emergency situation

6.5 Identify the role of the security operative in relation to first aid incidents

6.6 Recognise evacuation principles

This module includes the following interactive activities:

Key task 6

An emergency is any unexpected situation that is so serious that it must be dealt with immediately

It is important that all security operatives know how to deal with emergencies promptly, efficiently and safely.

174
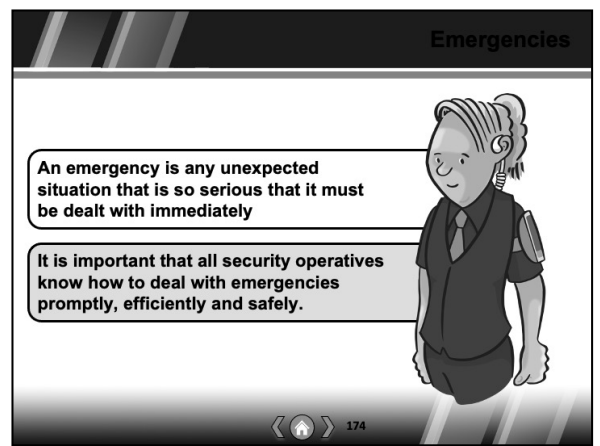
Emergencies

An emergency is any incident/situation that is unexpected and serious, that could threaten safety or cause serious disruption and therefore requires immediate attention.

Security operatives may come across or could be called to any number of serious incidents in the workplace, and it is important that they know how to deal with them promptly, efficiently and safely.

Emergencies can include incidents, occurrences
and accidents:

- an incident/occurrence could include a fight, power cut
  or drug overdose
- an emergency could include health emergencies such
  as epileptic seizure, anaphylactic shock, heart attack etc.
- an accident could include someone falling down steps
  or slipping on a wet floor.

Emergencies

Emergencies can include:

- incidents

- occurrences

- accidents

an incident/occurrence could include:

- a fight, power cut or drug overdose

an emergency could include health

- emergencies such as epileptic seizure, anaphylactic shock, heart attack etc.

an accident could include someone

- falling down steps or slipping on a wet floor

Incidents generally fit into 3 camps:

EMERGENCIES

URGERT

NON-URGERT

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

We can place incidents generally into three camps:

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

Emergencies that security operatives may become involved in include:

- power system/equipment failures
- floods
- actual or threatened serious injuries
- serious Illness
- fights/assaults
- bomb/terror threats
- gas leaks
- fires
- chemical spillages.

Types of emergencies and the actions to be taken

Examples of emergencies that security operatives may become involved in include:

- power system/equipment failures

- floods

- actual or threatened serious injuries

- serious illness

- bomb threats

- fires

- terror threats

All incidents need to be dealt with immediately and will often require the emergency services to be contacted.

Fires - Floods - Power cuts - Gas leaks - Chemical spillages

1 Activate the alarm

2 Evacuate the site

3 Call the emergency services on 999.

FIRE BELL

178

Fires, floods, power cuts, gas leaks and chemical spillages are normally dealt with by activating the alarm and then evacuating the site. The emergency services should be called once the evacuation has been started.

Actions – gas leak

If a gas leak is suspected, security operatives should try to ensure that no one smokes or switches on any lights or electrical equipment in the area

Even a small spark could cause an explosion

Where possible, doors and windows should be opened to try to disperse the gas

If possible, the gas supply should be turned off at the mains.

179

In a situation where a gas leak is suspected, once the evacuation has been started security operatives should try to ensure that no one smokes or switches on any lights or electrical equipment in the area, as even a small spark could cause an explosion. Where possible, doors and windows should be opened to try to disperse the gas. If possible, the gas supply should be turned off at the mains.

Road traffic accidents are usually dealt with by the police

Incidents of violence may be dealt with by removing the instigators from the site, calling the police or making arrests

First aid may also be required.

180

Road traffic accidents are normally dealt with by the police. An ambulance may also be required if serious injuries are sustained.

Incidents of violence may be dealt with by removing the instigators from the site, by calling the police or by making arrests if serious injuries are sustained. First aid may also be required.

All bomb threats and suspicious packages must be dealt with seriously by:

- raising the alarm
- evacuating staff and visitors/customers
- call the police.

It is important that all security operatives know and follow correct procedures for any of these emergencies. You need to ensure your own safety as well as the safety of others in dangerous situations. You may need to call and assist any of the emergency services.

You will need to take control of situations professionally and calmly and follow the correct procedures so that other people do what is safest and best for themselves until the situation is resolved.
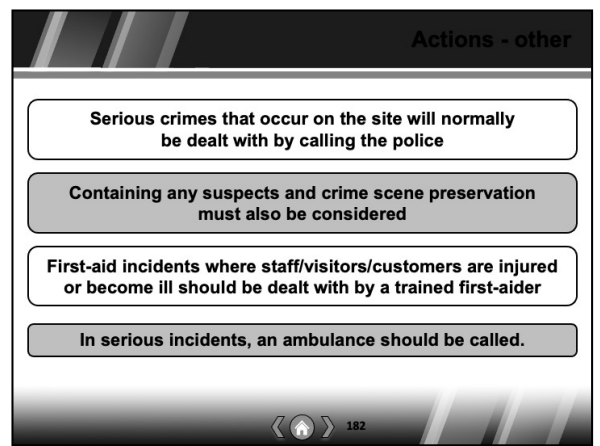
Serious crimes that occur on the site will normally be dealt with by calling the police

Containing any suspects and crime scene preservation must also be considered

First-aid incidents where staff/visitors/customers are injured or become ill should be dealt with by a trained first-aider

In serious incidents, an ambulance should be called.

Serious crimes that occur on the site will normally be dealt with by calling the police. Containing any suspects and crime scene preservation must also be considered.

First-aid incidents, where staff or visitors/customers are injured or become ill, should be dealt with by a trained first aider. In serious incidents an ambulance should be called.

If you need to call for the emergency services, call 999. This will put you through to the emergency services operator.

The operator will ask you for the following information:

- which service you require (police, fire, ambulance)
- the telephone number you are calling from (in case you are cut off or for a call back)
- your exact location (address and postcode)
- type of incident
- number of casualties
- extent of injuries
- any other dangers or hazards

Fight or flight

It is important that learners understand what happens to themselves and others when confronted by either conflict or frightening/threatening situations. Only then can they plan what is the best way to react and how to treat others when conflict arises.

If someone becomes angry and starts to threaten a security operative, the security operative will automatically start to use the emotional side of their brain more than the rational side. It is the natural human response to a threat/potential threat to wellbeing and safety.

If, as humans, we did not get frightened in such situations, our brains and bodies might not be prepared to be able to react quickly enough or in the proper way if we did actually need to protect ourselves.

When we become frightened our bodies will automatically go into what is called **fight or flight** mode. This is because of the basic natural animal instinct in us all to help us to survive potentially dangerous situations.

Fight or flight prepares our brains and bodies to:

• stand and physically fight off an attack (**FIGHT**)
• run away from the situation to keep ourselves safe (**FLIGHT**)

Advise the learners that during fight or flight, their bodies will release the hormone adrenaline into their systems to increase their physical ability to fight or run away. This adrenaline rush will increase their heart rates, pumping extra blood and oxygen to the muscles they need to use.

During fight or flight, eyes will widen to take in as much of the situation as possible, although sometimes attention will be centred directly onto the threat itself, causing what is often called tunnel vision.

Sense of hearing also intensifies, again to try to allow in as much information about the threat as possible.

Once the situation ends, your brain and body begins to calm down again in an attempt to get back to normal

Your body slowly returns to its natural relaxed state, and as you calm down, your brain returns to thinking with the rational side again.

186
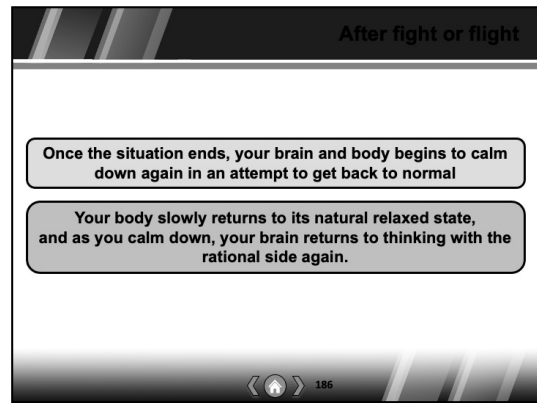
Once the situation ends, whether that is by the security operative having halted or fought off the threat, or whether they have been able to get away from it, their brain/body will begin to calm down again in an attempt to get back to normal.

Their body will slowly return to its natural relaxed state and as they calm down, their brain will return to thinking with the rational side again.

If brains and bodies do not return to their natural conditions as they should, you can go into a state known as shock

This normally only happens after a particularly threatening or frightening situation.

However, if our brains and bodies do not return to their natural conditions as they should, then we can go into a state known as shock. This normally only happens after a particularly threatening or frightening situation though.

Companies will often have an escalation procedure for incidents and emergencies. It is important that you:

- understand how a graduated response can be applied in each situation
- be required to record your involvement as you may be asked to review and evaluate the responses during the incident

> **When dealing with an emergency situation you must be aware of taking control in crowds to avoid people from being crushed or injured during an evacuation or invacuation.**

First aid is defined as the initial or immediate assistance given to someone who has been injured or taken ill, prior to the arrival of an ambulance, doctor or other suitably qualified person.

The main aims of first aid are to:

• preserve life

• prevent the condition from worsening

• promote recovery

• obtain qualified assistance

Person injury responses

You need to know:

- the site's policy for providing first aid
- what you are expected to do in a medical emergency
- who the designated first-aiders on the site are
- how to contact them
- where the first-aid room and equipment are

> You may even be required to undergo first-aid training.

191

As a security operative you must know your site's policy for providing first aid, you must know what you are expected to do in a medical emergency, and you must know who the designated qualified first aiders are on the site. You may even be required to undergo first-aid training yourself.

If you are trained to do so, you may be required to administer first aid in times of emergency

Remember the following:

- ensure your own safety first
- assess the situation
- control the situation
- diagnose the injury/illness
- save life
- send for appropriate medical assistance
- keep people safe
- provide privacy.

192

If you are trained to do so you may be required to administer first aid in times of emergency. If you are, remember the following:

- ensure your own safety first

- assess the situation

- control the situation

- diagnose the injury/illness

- save life

- send for appropriate medical assistance

If you are not trained to administer first aid in times of emergency

Remember the following:

- call the first-aider if you are not qualified
- know when to call an ambulance
- ensure that onlookers are kept to a minimum but also monitor anyone who has remained for signs of shock
- provide as much of a physical block as you can, to protect the dignity of the casualty and prevent onlooking
- direct the ambulance to the casualty (if you are not the first-aider).

193

- call the first-aider if you are not qualified (if you are, you may still need support)
- know when to call an ambulance; you or the first-aider may be able to deal with a minor injury, but it is very important that you know when to call an ambulance - always take guidance from a qualified first-aider
- ensure that onlookers are kept to a minimum but also monitor anyone who has remained for signs of shock
- provide as much of a physical block as you can, to protect the dignity of the casualty and prevent onlooking
- direct the ambulance to the casualty (if you are not the first-aider)

Recording first-aid incidents

It is important to record all details relating to injuries sustained on the site, whether they are sustained through accidents or criminal actions

The information contained in the accident book can often help employers to:

- identify accident trends
- improve the general health and safety of the site
- assist with insurance and/or criminal investigations.

194

As mentioned previously, it is important to record all details relating to injuries sustained on the site, whether they are sustained through accidents or criminal actions.

The information contained in the accident book can often help employers to identify accident trends and improve the general health and safety of the site. These records may also be required for insurance and/or investigative purposes.

Evacuation is the controlled process of emptying an area or premises of people

Evacuation:

- can be to an adjoining area or premises depending on the incident
- may be required in the event of flooding, fire or terror threat.

Invacuation is the controlled process of getting people into safe premises due to an incident which could cause harm to people who are outside

- Invacuation may be required if a person with a firearm started to shoot people in the street
- Security operatives should encourage everyone into the building and lock the doors for safety

Different sites or venues may have different evacuation and invacuation procedures. You will need to make yourself aware of these policies.

1 What are the FOUR aims of first aid?

1 ....

2 ....

3 ....

4 ....

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

1 **What are the FOUR aims of first aid?**

1 **Preserve life**

2 **Prevent the condition from worsening**

3 **Promote recovery**

4 **Obtain qualified assistance.**

(2) **Identify FOUR types of emergency that could happen in the workplace.**

1 ....

2 ....

3 ....

4 ....

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

(2) **Identify FOUR types of emergency that could happen in the workplace.**

1 Power system or equipment failures

2 Floods

3 Fire

4 Terrorist threats.

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

3 **Explain the principles of evacuation and invacuation.**

Evacuation	Invacuation
A controlled process of emptying an area or premises of people	A controlled process of getting people into a safe premises due to an incident that could cause harm to people who are outside.

Communicate effectively

Module 1:7

Completion of this module will enable learners to meet the following learning outcome:

Learning outcome 7: Understand how to communicate effectively as a security operative

This includes assessment criteria:

7.1 Identify the different types of communication

7.2 State the importance of effective communication

7.3 Identify the benefits of teamwork in the private security industry

7.4 State the principles of customer service

7.5 Recognise diverse customer needs and expectations

This module includes the following interactive activities:

• group exercise – the make-up of communication (discussion)

Key task 7

You will regularly come into contact with members of the public during the course of your duties

You will also regularly interact with other members of staff and people from other organisations

Effective communication is vital.

204

Communication

Security operatives will regularly come into contact with members of the public. They will also regularly interact with other members of staff and people from other organisations and therefore need to have effective communication skills.
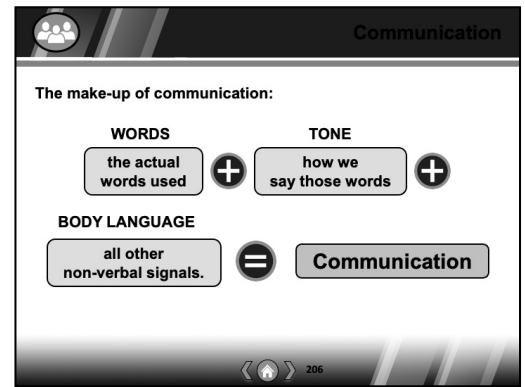
How we communicate

How we communicate

Communication is the sending and receiving of signals

- The 'sender' decides what thoughts they wish to pass on, 'encodes' those thoughts into the most effective form of communication and then 'sends' those thoughts to the 'receiver'
- The receiver takes in the message and replies if necessary
- Receiver and sender check understanding.

SENDER

ENCODES THOUGHTS

SENDER SENDS

RECEIVER RECEIVES

205
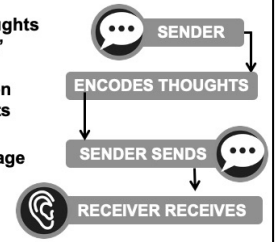
How we communicate

SENDER – ENCODES THOUGHTS – SENDER SENDS – RECEIVER RECEIVES

The make-up of communication:

WORDS		TONE	
the actual words used	➕	how we say those words	➕

BODY LANGUAGE

all other non-verbal signals. ➖ **Communication**

Group exercise - the make-up of communication

- **WORDS - the actual words used   7%**

- **TONE - how we say those words   38%**

- **BODY LANGUAGE - all other non-verbal signals 55%**

The actual percentages are disputed from theory to theory. Discuss with your groups whether you think the percentages are accurate or nonsense.

Verbal communication is when you interact with another person using words and tone to convey your message

The words you use are important, but so is the tone in which you use those words.

Verbal communication is the use of words and tone to convey a message when interacting with another person.

Remind learners that while the words they use are important, so is the tone they use to express those words - it's not just what you say, but how you say it that counts.

Verbal communication includes:

• speaking

• listening

• reading (aloud)

• pitch and tone of voice

Non-verbal communication is everything else that you do when you communicate with another person on a face-to-face basis

How you stand, what you are wearing, how close you are to the other person, facial expressions, eye contact, how you use your hands, other physical gestures – these all help you to convey your message.

Non-verbal communication is everything else that people do when communicating with another person on a face-to-face basis.

Non-verbal communication includes:

• gestures

• stance

• eye contact

• facial expression

• written communication (pictures, signs, script, text messages etc.)

To effectively communicate in the workplace you will need to:

- **choose an appropriate medium and use appropriate language for the message and recipient it is intended for**
- **deliver the message clearly**
- **check the recipient's understanding of the message, for example by asking them to repeat the message back to you**

Communicating effectively will also help to prevent misunderstandings.

Communicating effectively will also help to:

● prevent misunderstandings
● prevent mistakes being made
● reduce incidents of conflict, aggression or violence

Security operatives need to come across as positive, assertive and professional at all times if they are to be treated with respect by anyone they come into contact with.

- Effective communication in a team is essential
- Communication skills play an important role in how you interact with your colleagues, supervisors and managers
- You should treat all members of staff with courtesy and respect and you should expect to be treated in the same way.

211

Effective communication in a team is essential

Good teamwork in the workplace:

- promotes safety
- provides a professional and safe service and establishment
- supports colleagues
- promotes efficiency.

212

Diverse customer needs

All customers are different people, with differing needs and expectations

People form their own personal values as they grow up

Security operatives need to take into account other people's values and try to choose the most appropriate and effective way of dealing with them.

213

Diverse customer needs

All customers are different people, with differing needs and expectations. Customers may:

- come from different countries
- have different faiths/religions
- be from different age groups
- have different levels of physical/mental ability

People form their own personal values as they grow up. The following factors all contribute to how a person's values are formed:

- where they were born
- where they live
- how they were brought up
- their friends and family
- their jobs

Security operatives need to factor in the above and based on this, choose the most appropriate and effective way to deal with each particular customer.

For example, security operatives would speak to a distressed young child in the street very differently to the way they would treat a drunk, aggressive customer outside a pub. Both are customers if they have to be dealt with as part of their duties, but both would need to be dealt with differently because of their different values, needs and expectations.

Consider the Jamie Bulger case (child who was tortured and killed by other children) or any other example you prefer.

Customers with particular needs

You may need to consider adapting to how you would communicate with individuals who have particular needs such as:

- physical disabilities
- learning difficulties
- sensory impairment
- English as a second language
- being under the influence of drink and drugs

You may need to speak slower when giving information, assistance or directions or draw a picture to provide guidance

Remember it is important to acknowledge and respect all individuals.

One main role of a security operative is looking after people

How people are treated is very important. Customer care is all about delivering service and providing security to customers on a day-to-day basis.

Examples of delivering good customer care include:

- being professional with every customer
- being approachable
- communicating with them effectively
- acknowledging them
- concerning yourself with customers' needs
- building a rapport
- treating customers as you would wish to be treated yourself
- going out of your way to help customers
- leaving customers pleased with how you have dealt with them.

Good customer service can often avoid problems occurring even if the problems haven't been caused by you or are out of your control

To appease the customer in these circumstances you can:

- acknowledge and listen to them
- establish the customers' need
- put yourself in the customer's position
- accept responsibility for the problem
- involve the customer in the proposed solution
- see it through, make sure any promised actions are carried out.

Security operatives must understand that every single person they come into contact with is a customer

Security operatives provide customer service to both internal and external customers (direct and indirect).

Internal customers

Internally, within your own company, your customers include your work colleagues, supervisors, managers and anyone working for any other company or organisation on the site

External customers

Other customers you may come into contact with include visitors to the site, workmen, delivery drivers, the emergency services, neighbours and members of the public.
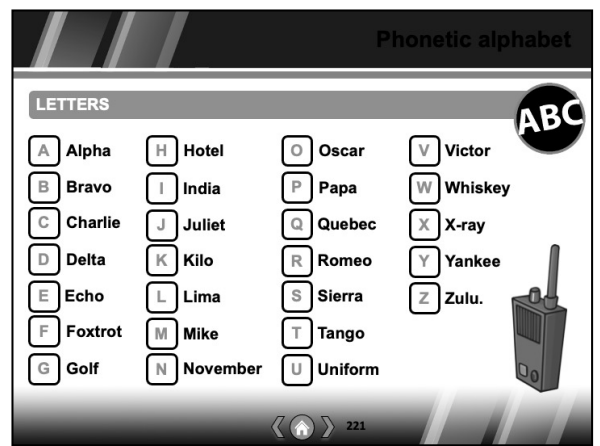
The phonetic alphabet

In the phonetic alphabet, all the words used to represent the letters sound different, so there is no confusion about what people are saying.

Security operatives may need to use the phonetic alphabet during the course of their duties, as they may well have to use the telephone or radio to communicate with other members of staff, outside organisations or members of the public.

It is important that this is always done professionally and politely and that security operatives always remember to use clear language.

Effective telephone/radio communication between security teams and other people on-site is essential and helps to deal with incidents swiftly and efficiently.

LETTERS

A Alpha	H Hotel	O Oscar	V Victor
B Bravo	I India	P Papa	W Whiskey
C Charlie	J Juliet	Q Quebec	X X-ray
D Delta	K Kilo	R Romeo	Y Yankee
E Echo	L Lima	S Sierra	Z Zulu.
F Foxtrot	M Mike	T Tango	
G Golf	N November	U Uniform	

ABC

221

Try asking the learners to spell another person or their own name phonetically.

LETTERS
A – Alpha
B – Bravo
C – Charlie
D – Delta
E – Echo
F – Foxtrot
G – Golf
H – Hotel
I – India
J – Juliet
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 – X-ray
Y – Yankee
Z – Zulu

NUMBERS
0 – Zero
1 – Wun
2 – Two
3 – Tree (three)
4 – Fower (four)
5 – Fife (five)
6 – Six
7 – Seven
8 – Ait (eight)
9 – Niner (nine)

① Provide THREE examples of verbal and non-verbal communication.

Verbal	Non-Verbal

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

1 **Provide THREE examples of verbal and non-verbal communication.**

Verbal	Non-Verbal
Speaking, pitch and tone of voice, listening	Gestures, stance, eye contact.

Key Task 2

2 **Give THREE examples of good customer service.**

1 ....

2 ....

3 ....

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

2 **Give THREE examples of good customer service.**

1 Being professional with every customer

2 Being approachable

3 Communicating effectively.

③ **State the importance of effective communication in the workplace.**

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

3 State the importance of effective communication in the workplace.

Helps to successfully get the job done and ensures all people receive a good impression of you.

Record keeping

Module 1:8

228

Completion of this module will enable learners to meet the following learning outcome:

Learning outcome 8: Understand record keeping relevant to the role of the security operative

This includes assessment criteria:

8.1 State the importance of accurate record keeping

8.2 Identify the types of records that may need to be completed

8.3 Identify what information to include in records

8.4 Demonstrate the accurate completion of an evidential statement (Section 9 Statement)

8.5 State the process of attending court to give evidence

This module includes the following interactive activities:

• class question: Why is accurate record-keeping important?

Key task 8

Class question: Why is accurate record-keeping important?

- You may need to refer back to an incident months or years after the event
- Memories can alter with time, particularly when an incident is discussed with others

Typical records you may complete include:

- incident reports
- accident records
- searches and checks
- logbooks
- pocket notebooks
- search/visitor/ key registers
- duty sheets

- lost/found property registers
- message books
- handover reports
- other site specific reports.

Types of reports will vary from company to company

Security operatives need to ensure that they know what records they are required to use at their venues, where they are kept and how to complete them.

These various reports provide a permanent written record of incidents that have happened and can be used to refresh security operatives' memories prior to giving evidence in court.

They can also be used to assist the site/venue to comply with the law, assist outside agencies, protect security operatives from malicious allegations and can help to justify any actions they have taken.

REMEMBER

A	ACCURATE
B	BRIEF
C	CLEAR

All communications should be accurate, brief and clear.

Incident reports

Records need to be completed as soon as possible following the incident. They should be purely factual, without personal opinion and each separate report should be signed, dated and timed.

- Notebooks are still official documents
- Must be used properly at all times
- Only be used to record work-related matters
- For making accurate, timely notes while working at the scene
- Ensure that sufficient details about a routine or unusual event are taken at the time
- Fuller report can be made of the incident later
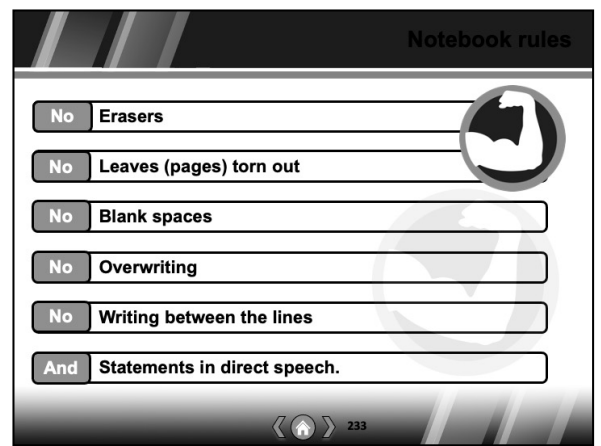- Must be kept securely as they may contain confidential information.

Using notebooks

While full incident reports can be completed in the relative comfort of an office or staffroom, there are occasions when security operatives may need to make accurate, timely notes while working at the scene of an incident.

To ensure that sufficient details about a routine or unusual event are taken at the time, door supervisors will often need to use notebooks.

A fuller report can be made of the incident later, using the information in the notebook taken at the time.

No	Erasers
No	Leaves (pages) torn out
No	Blank spaces
No	Overwriting
No	Writing between the lines
And	Statements in direct speech.

Notebooks need to be completed in black ink and notebook rules should apply.

The mnemonic '**NO ELBOWS**' is a useful way of understanding and remembering the general rules for when using notebooks:

No **E**rasures

No **L**eaves (pages) torn out

No **B**lank spaces

No **O**verwriting

No **W**riting between the lines

and **S**tatements in direct speech

Incident reports will need to show:

- who - the report is for and who it is written by
- what - happened/action was taken/was the result
- when - day/time/date
- where - place of incident
- details of any other witnesses/people/injuries or property

Records need to be completed as soon as you are able to following the incident and should be purely factual, without personal opinion, and each separate report should be signed, dated and timed.

234

Reporting procedures

Basic information will always be required.

Statement:
A written account of what evidence a witness
can give about an incident

The rules about statement writing and giving evidence can be
found in the Police and Criminal Evidence Act (PACE) 1984.

Formal police statements are often referred to as a Section 9 statement.

NI: The Police and Criminal Evidence (Northern Ireland) Order 1989.

Statements are taken for the following reasons:

- to allow police officers to collate and evaluate evidence during investigations
- to record witnesses' evidence as soon as is practicable after an incident
- to submit as evidence (when not contested) in court to save the attendance of a witness
- to refresh a witness's memory prior to actually giving evidence in court.

- If security operatives are required to make a statement, the police will provide help
- They will ask questions about the incident
- Security operatives are entitled to write their own statements, but this is not recommended

If force is used against a person or while carrying out a lawful arrest, the incident will need to be explained in detail, including:

- time, date and location of incident
- how the security operative (SO) was called to the incident
- what type of incident it was
- if the SO was alone
- how the incident was approached
- what was seen and heard
- number of people involved
- the state of mind of the people involved.

- the offender's size in comparison to the SO
- how the SO felt about the situation
- actions that were taken
- what was said to the offender
- what was said to the SO
- why the SO decided to use force
- how much force was used
- what the level of resistance was
- how the offender was restrained or ejected
- how they were held until police arrived
- whether there were any injuries.

How the SO felt, e.g. frightened, in fear of being assaulted etc.

- details of the officer who took the offender from the SO
- details of any witnesses
- details of first-aid/medical support provided
- details of the support involved and any follow-up action required.

Descriptions of people may need to be given when providing a statement. Accurate information must be provided

- How long was the person observed for?
- How far away was the person from the SO?
- What were the lighting conditions like?
- Was the view impeded at any point?
- Has the SO seen the person before, if so how many times?
- Is there any special reason for remembering the person?

240

Identification in statements

Should security operatives be required to describe a person they have seen in a statement, as well as giving as complete and accurate a description as they can, they should also cover the following points:

• how long they observed the person for.

• how far away the person was from them.

• what the lighting conditions were like at the time.

• whether their view of the person was impeded in any way.

• whether they have ever seen the person before and if so, how many times.

• whether they had any special reason for remembering the person.

• if they subsequently identified the person to police, how much time passed between originally seeing them and the identification?

• any differences between the security operative's descriptions of the person and how they looked when they identified them to the police

Covering all of these points will provide
good evidence for the prosecution.

If security operatives cover all of these points in their statements, they will be providing good evidence for the prosecution where the case depends on the identification of the accused and shows a professional understanding of both the rules of evidence and the importance of proper descriptions and identification.

Attending court

- Courts are designed to intimidate the guilty, however this can also intimidate the witnesses and innocent parties

- Security operatives may refer to their notebooks, however the defence may also see the relevant entries

- Security operatives should always take the advice of their solicitors/CPS but only ever tell the truth

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

1 **Explain the importance of accurate record-keeping.**

To comply with the law

To provide a clear audit trail or the incident or accident

To prevent yourself from having to rely on your memory.

② **Identify the types of information that should be included in records.**

1	....	**4**	....
2	....	**5**	....
3	....	**6**	....

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

② Identify the types of information that should be included in records.

1	Day, date and time of incident	**4**	How you were alerted to it
2	What happened	**5**	What you saw
3	Where it happened	**6**	Details of any witnesses.

(3) Describe the process of attending court to give evidence.

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

3 **Describe the process of attending court to give evidence.**

Arrive at court in good time

Inform the CPS you have arrived and follow their instructions

Read through your statement

Stand in the witness box

Swear your oath

Answer the questions put to you honestly.

Completion of this module will enable learners to meet the following learning outcome:

Learning outcome 9: Understand terror threats and the role of the security operative in the event of a threat

This includes assessment criteria:

9.1 Identify the different threat levels

9.2 Recognise the common terror attack methods

9.3 Recognise the actions to take in the event of a terror threat

9.4 identify the procedures for dealing with suspicious items

9.5 Identify behaviours that could indicate suspicious activity

9.6 Identify how to respond to suspicious behaviour

This module includes the following interactive activities:

 Key task 9

Terrorism is the use of violence, threats and intimidation, especially in the pursuit of political aims.
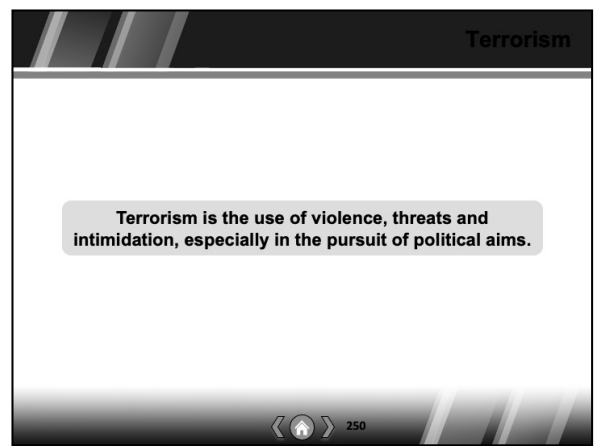
Terrorism

The use of violence, threats and intimidation, especially in the pursuit of political aims.

Security operatives need to be aware of:

- what is currently happening around the world and in their particular area
- any recent terrorist attacks or threats
- the location of their own site in relation to other possible targets nearby
- where the site itself is famous or important in its own right
- the vulnerability of the site to attack
- the current level of threat nationally.

Public, commercial and retail premises, as well as places of entertainment could all become targets of either bomb threats or actual terrorist attacks.
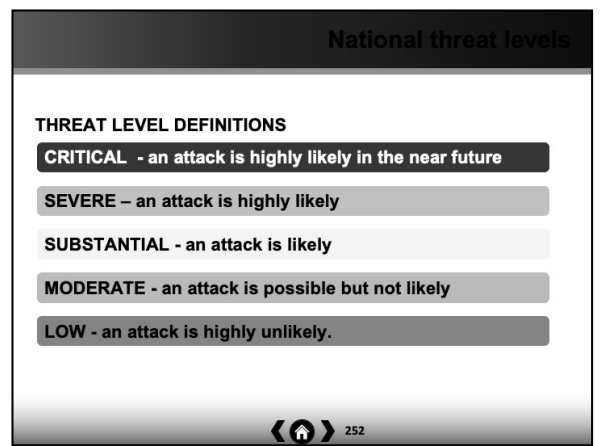
Security operatives need to be aware of:

- what is currently happening around the world and in their particular area
- any recent terrorist attacks or threats
- the location of their own site in relation to other possible targets nearby
- where the site itself is famous or important in its own right
- the vulnerability of the site to attack
- the current level of threat nationally

THREAT LEVEL DEFINITIONS

CRITICAL - an attack is highly likely in the near future

SEVERE – an attack is highly likely

SUBSTANTIAL - an attack is likely

MODERATE - an attack is possible but not likely

LOW - an attack is highly unlikely.

252

NATIONAL THREAT LEVEL DEFINITIONS:

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

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

- **SUBSTANTIAL** - an attack is likely

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

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

Threat levels themselves do not require specific responses, however it is important that security operatives are aware of the different response levels and what moving from one level to another means for the location they are working in and the plan that is in place.

www.mi5.gov.uk/threat-levels

Counterterrorism measures will help to reduce the chances of a site becoming a target. Threats can be reduced by:

- vigilance
- good housekeeping
- use of physical security measures
- regular, obvious patrols
- use of strict access control procedures
- effective search procedures
- visible use of CCTV
- the reporting of suspicions to supervisors or managers immediately
- know what information emergency response require and have an awareness of emergency response times.

Counterterrorism reduces the chances of a site becoming a target. Threats can be reduced if security operatives:

- are vigilant

- maintain good housekeeping

- use physical security measures

- carry out regular, obvious patrols

- implement strict access control procedures

- use effective search procedures

- visibly use CCTV

- report suspicions to supervisors or managers immediately

It is important to know what information emergency response require and have an awareness of emergency response times.

Once terrorists have identified a target, the potential attack will be moved into the planning phase. This phase involves:

- **gathering information on the target**
- **identifying the target's vulnerabilities**
- **identifying levels of security present at the target.**

By gathering information on the target, terrorists are able to decide their preferred method of attack.

The most current terrorist attack methods have included:

- marauding terror attacks (MTAs)
- explosive devices, including improvised explosive device (IED), person-borne improvised explosive device (PBIED), vehicle-borne improvised device (VBIED)
- vehicle as a weapon (VAAW)
- hazardous substances including chemical, biological and radiological (CBR)
- cyberattacks.

Attack methods can vary and there may be instances where periods of training and rehearsals may precede the actual attack.

Marauding terror attacks (MTAs) can include the use of firearms, knives, blunt objects etc.

Vehicle as a weapon (VAAW) is also known as vehicle ramming.

The role you will be expected to take during a terror attack will be outlined in your organisation's policies and procedures

You should encourage members of the public to:

RUN	HIDE	TELL
to a place of safety	if you cannot run, hide	call 999 (response times may vary according to location).

In the rare event of a terror attack, security operatives should encourage members of the public to:

- **RUN** – to a place of safety
- **HIDE** – if you cannot run, hide
- **TELL** – call 999 (response times may vary according to locations)

In the event of an attack, you should:

- consider your route
- insist others go along with you (however, don't let their indecision slow you down)
- once you have identified a safe route, RUN

Consider your route as you leave. Will it place you in the line of fire, is it safer to wait for the attacker to move away before you continue?

If you can't move to safety - HIDE

When finding a hiding place, you should consider:

- the exits and escape routes
- rooms that have reinforced walls and doors with internal locks
- moving away from the door
- switching your phone to silent and switching off vibrate
- staying silent (don't shout for help).

If you are able to evacuate, get as far away as possible and TELL

Call the police by dialling 999

- **TELL them clearly where you are located and where the attackers are**
- **Give a clear description of the attackers, including details of their clothing and weapons**
- **Give details about the number of casualties**
- **Explain the layout of the building**
- **Include anything else that you think is important.**

Tell

If able to evacuate the premises, security operatives should stop others from entering and get as far away from the danger as possible (but only if this does not put them in danger).

Follow all invacuation/lockdown and evacuation procedures

Invacuation/lockdown -

staff members and members of the public should be moved to the most sheltered area of the venue/site, away from windows and other exposed areas. All external doors and windows should be locked

Evacuation -

the orderly removal of staff and members of the public to a safe place away from the immediate vicinity of the building. Evacuation will normally happen in situations such as a fire.

An early assessment of the situation is vital. If a terrorist attack begins outside, a quick lockdown procedure could protect everybody inside the site/venue

If lockdown is slow, incomplete or causes a state of confusion, the threat could move inside, putting the people inside at great risk.

261

Following procedures during an attack can help preserve life.

	Pros	Cons
Invacuation	Locks staff and members of the public away from the perpetrator, providing a physical barrier	Potential lack of exits limits the ability to run should the perpetrator gain access or the attack zone spreads
Evacuation	Allows staff and members of the public to get as far away as possible from the scene of the incident	Some evacuation routes may put staff and members of the public at risk of being in the line of fire, or the perpetrator may attempt to pursue along the evacuation route.

Pros and cons for invacuation and evacuation

You need to be aware of suspicious packages and know the procedures to follow if one is identified

You need to know what looks out of place at the venue or site that you are working at

You can use the HOT protocol to help you determine whether items are suspicious.

H HIDDEN – has someone deliberately tried to conceal it from view?

O OBVIOUSLY SUSPICIOUS – does its appearance seem odd or out of the ordinary? Maybe it's even showing wires, batteries or liquids?

T TYPICAL – is it typical for the location? For example, ae large rucksack would be expected at an outdoor festival but would be out of place at an indoor concert venue.

Suspicious items should be treated with caution

- Don't touch the item
- Move yourself and others a safe distance from the item
- Clear 100m around the object
- Large items or small vehicles need a clear area of around 200m
- Large vehicles need a clear area of 400m or the length of a football pitch.

Safety distances:

- distances v suspicious item size:
  - small items: 100m
  - large items or small vehicles: 200m
  - large vehicles: 400m or the length of a football pitch

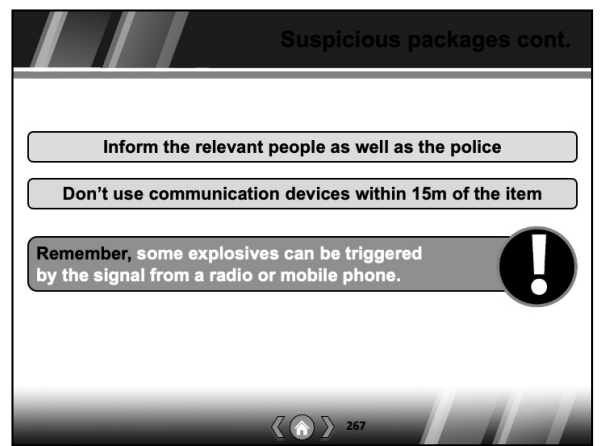How to visually represent safety distances e.g. football field/London bus.

Keep yourself and others out of line of sight

If you can't see the item then you're better protected from it

THINK ABOUT
what you can hide behind, find something
substantial and keep away from glass, such
as windows and skylights.

?

Inform the relevant people as well as the police

Don't use communication devices within 15m of the item

Remember, some explosives can be triggered by the signal from a radio or mobile phone.

267

Inform relevant people:

• manager

• supervisor

• the police

Don't use radios or mobile phones around suspicious packages as they may trigger explosives . Keep a distance of 15m when using communication devices.

Remember the 4 Cs:

1 Confirm if the package is suspicious

2 Clear the area as best you can

3 Communicate to your team and the police

4 Control others getting into that area.

The four C 's:

- Confirm
- Clear
- Communicate
- Control

Suspicious activity is any observed behaviour that could indicate terrorism or terrorism-related crime.

Security operatives need to be familiar with the different methods of observing suspicious activity, including:

- people
- places
- vehicles
- locations

Hostile reconnaissance is the term used to describe how terrorists gain information on potential targets

They will often:

- visit potential targets a number of times prior to an attack
- try to find out as much as they can about the location itself
- try to discover the best time and method of attack

You need to be vigilant at all times to try and recognise suspicious behaviour that may indicate a terrorist interest in your site.

270

You should use your customer service skills to disrupt potential hostile reconnaissance, having a professional, visible presence is a tool that all security operatives can use to deter hostile reconnaissance.

Suspicious behaviour may include:

- a particular interest in the outside of the site
- an interest in the CCTV systems
- taking pictures of the site (overtly or covertly)
- making notes or drawing diagrams of the site
- taking an interest in the timings of activities
- false alarm activations (testing response times)
- damage to perimeter security
- attempts to disguise identity (hats and hoods)
- trespassing or loitering with no good reason
- asking unusual/specific questions about the site or security arrangements
- nervousness
- reluctance to be noticed or seen
- use of forged/fake identity documents
- strangely parked vehicles.

Suspicious behaviour may also include:

- an interest other security measures that are in place (as well as CCTV)

- parked vehicles with people inside

- empty parked vehicles left unattended for long periods

- making unusual requests for information

- individuals avoiding security staff

- breaching restricted areas

- inappropriately dressed for the season/location

- individuals carrying out activities inconsistent with the nature of the building or area

- multiple sightings of the same suspicious person, vehicle or activity

- carrying large amounts of cash

Don't be afraid to take action, have the confidence to ACT

Dial 999 if it is a life-threatening emergency and provide the operator with the following information:

- your place of work and the specific building
- location of the suspicious package inside the building
- whether all customers and employees have been evacuated from the building.

Non-urgent information about terrorism should be passed to the anti-terrorist hotline on
0800 789321

This line is covered at all times by specialist counterterrorism police officers
- Urgent information should be passed on using 999
- Report online https://act.campaign.gov.uk/
- non-emergency, call 101.

273

- Non-urgent information about terrorism should be passed to the anti-terrorist hotline on 0800 789321. This line is covered all the time by specialist counterterrorism police officers
- Urgent information should be passed using the 999 system
- Report online https://act.campaign.gov.uk/
- Non-emergency, call 101

See it

Say it

Sorted

The British Transport Police's nationwide campaign, designed to encourage train passengers and people visiting train stations to report any unusual items or activity. Passengers and visitors can report any issues by texting **61016** or by calling **0800 405040**.

See, Check and Notify

A current awareness strategy that aims to help businesses and organisations maximise safety and security using their existing resources

Action Counters Terrorism (ACT) Awareness - elearning

This is a free course to access via:

https://ct.highfieldelearning.com/

Current initiatives

- See, Check and Notify is a current awareness strategy that aims to help businesses and organisations maximise safety and security using their existing resources.

- ACT awareness e-learning has been developed to support the United Kingdom's strategy for countering terrorism. This e-learning provides nationally recognised corporate CT guidance to help people better understand and mitigate against counter-terrorist methodology. ACT e-learning https://ct.highfieldelearning.com/

Additional information, advice and guidance can be found with the following sources:

Centre for the protection of National infrastructure (CPNI)
www.cpni.gov.uk/cpni-context

National Counter Terrorism Security office (NaCTSO)
www.gov.uk/government/organisations/national-counter-terrorism-security-office.

276

For additional support and guidance, signpost to:

- CPNI website
- NaCTSO website

ACT | ACTION COUNTERS TERRORISM

1   **What are the FIVE different threat levels?**

1	....	**4**	....
2	....	**5**	....
3	....		

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

1 **What are the FIVE different threat levels?**

1 Critical

2 Severe

3 Substantial

4 Moderate

5 Low.

② **What are the most common terror attack methods?**

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

2 What are the most common terror attack methods?

Marauding terror attack

Explosive devices

Vehicle as a weapon

Hazardous substances

Cyberattacks.

3 Identify behaviours that could indicate suspicious activity and explain how you would respond to the activity you have identified.

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

③ Identify behaviours that could indicate suspicious activity and explain how you would respond to the activity you have identified.

Particular interest in the outside of the building

An interest in the CCTV systems and other security measures

Asking unusual questions or very specific questions about the site or security arrangements.

283

This list is not exhaustive.

In all cases report to line manager, supervisor or venue manager or use the confidential anti-terrorist hotline.

If life threatening call 999.

Keeping vulnerable
people safe

Module
1:10

284

Completion of this module will enable learners to meet the following learning outcome:

Learning outcome 10: Understand how to keep vulnerable people safe

This includes assessment criteria:

10.1 Recognise duty of care with regard to vulnerable people

10.2 Identify factors that could make someone vulnerable

10.3 Identify actions that the security operative should take towards vulnerable individuals

10.4 Identify behaviours that may be exhibited by sexual predators

10.5 Identify indicators of abuse

10.6 State how to deal with allegations of sexual assault

10.7 State how to deal with anti-social behaviour

This module includes the following interactive activities:

• class question: What behaviours might indicate a sexual predator?

• class question: What behaviours might indicate abuse?

• class question: What is anti-social behaviour?

Key task 10

Security operatives have a duty of care for all individuals on their premise but particularly for vulnerable people

Duty of care is defined as:
'a moral or legal obligation to ensure the health, safety and welfare of others.'

It can be difficult to tell who is and who is not vulnerable, so best practice is to have a duty of care for everyone.

Discuss the difference between moral and legal obligations and when they might apply.

Employers have a moral and legal duty under the Health and Safety at Work etc. Act 1974.

Vulnerable people may be:

- under the influence of drink or drugs
- alone or receiving unwanted attention
- separated from friends
- appearing lost or isolated
- being followed or threatened
- victims of domestic violence
- young people under the age of 18
- being elderly.

Vulnerable people

As part of customer service and their roles in protecting people from harm, security operatives need to be aware of any people who may be classed as vulnerable (people who may be at more risk of harm than others).

Security operatives need to carefully consider the implications for vulnerable children and young adults either passing or leaving venues/sites. They need to consider whether they require medical attention, whether they have friends/family nearby and whether they have all of their belongings with them.

They need to question whether they appear to fit into any of the above categories.

Security officers need to look out for the following behaviours from vulnerable people under the following categories:

- **drink/drugs** – reduced inhibitions, over-friendly, uncoordinated, aggressive, inability to make informed decisions, unaware of own abilities/limitations
- **alone/unwanted attention** – distressed, being followed/threatened

Vulnerable people may also:

- have mental ill health
- have learning disabilities
- have physical disabilities
- be elderly
- be acutely ill
- have invisible disabilities.

287

Invisible disabilities – physical, mental or neurological conditions that limit a person's movement, senses or activities that are invisible to the onlooker.

Consider

- Is there a relative or friend nearby to help them?
- Can you telephone anyone to come and help them?
- Are there any local safe havens or safety initiatives nearby?
- Can local street marshals, street pastors or similar groups help them?
- Do you need to call the emergency services?

If in any doubt whatsoever, report as soon as possible to your supervisor, the police or call crimestoppers.

288

Actions towards vulnerable people

In your professional judgement, if they appear to be vulnerable, you need to consider what help they might need.

Local safe havens/safety initiatives – e.g. those run by St John Ambulance or 'Ask Angela'.

There are certain indicators that a child is being sexually exploited such as:

- children and young people in the company of older people or antisocial groups
- acting in an inappropriate and sexualised way
- being intoxicated arriving and departing a location with
- different adults
- getting into and out of several different cars

You must be vigilant at all times if you suspect a child is being sexually exploited, you must report it immediately and follow the organisation's policies and procedures.

Sexual predators are those who commit sexual crimes

They very often target vulnerable children, young adults or adults they think they can groom or overpower

They can be all genders, shapes and sizes

They will often appear to be confident, friendly, helpful and sober.

Effective sexual predators do not seem to be a predator to the victim.

Sexual predators may select their victims based on:

- gender
- age
- race
- vulnerability
- appearance
- location
- time of day.

Sexual predators may have a preference as to who they target.

This may be a sexual preference alone or an additional factor such as young or intoxicated.

What behaviours might indicate a sexual predator?

- Close monitoring of vulnerable people
- Buying drinks for already drunk individuals
- Buying gifts for vulnerable people
- Suspicious behaviour around certain times and venues
- Inappropriate use of technology.

292

Class question: What behaviours might indicate a sexual predator?

Sexual predators

Security operatives must be able to identify the behaviours that may be exhibited by sexual predators.

It is important that learners remember that sexual predators don't look just one particular way, but are all genders, shapes and sizes.

Re. buying gifts for vulnerable people – sexual predators may give gifts to those in poor/unsettled homes, e.g. offering to share a gaming console with a financially poor person or offering refuge during a divorce.

Re. suspicious behaviour around certain times/venues – venues could include schools/play areas/pubs/clubs etc.

Re. inappropriate use of technology – predators could use phones, for example, to upskirt (taking a photograph underneath a woman's skirt/dress without her consent).

- Restricting the freedom of an individual
- Unexplained bruising
- Lack of confidence and insecurity
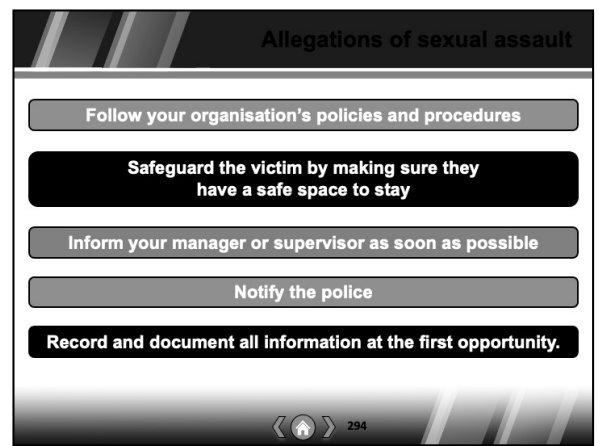- Change in circumstance, e.g. cleanliness/appearance.

Class question: What behaviours might indicate abuse?

Indicators of abuse

Abuse can be mental as well as physical, so an abuser may be able to both mentally and physical restrict an individual's freedom.

Unexplained bruising may be clearly visible to security operatives, however individuals may be able to keep their bruises/injuries hidden.

Security operatives may be able to pick up on a change in personality/circumstance from a regular customer or colleague which could be indicating that mental or physical, or both types of abuse are occurring. Changes in personality/circumstance could be for the better or worse.

Follow your organisation's policies and procedures

Safeguard the victim by making sure they
have a safe space to stay

Inform your manager or supervisor as soon as possible

Notify the police

Record and document all information at the first opportunity.

294

Allegations of sexual assault

Security operatives regularly wear uniforms. Some people find this reassuring and may choose to tell the operative about the abuse that they have been subjected to. This is called a disclosure.

Every organisation has a policy on what action to take if a member of staff or customer discloses information to them. Security operatives must follow the procedures when dealing with allegations of sexual assault. They must in the first instance:

- safeguard the victim by making sure they have a safe space to stay that is separate from the assailant
- inform their manager/supervisor as soon as possible
- notify the police
- record and document all information at the first opportunity

There are 3 main categories for anti-social behaviour, depending on how many people are affected

1 Personal antisocial behaviour - when a person targets a specific individual or group

2 Nuisance antisocial behaviour - when a person causes trouble, annoyance or suffering to a community

3 Environmental antisocial behaviour - when a person's actions affect the wider environment, such as public spaces or buildings.

295

Class question: What is anti-social behaviour?

Anti-social behaviour

Security operatives should always try to be positive and productive in their attitudes when dealing with members of the public that are demonstrating anti-social behaviour.

- Source https://www.thamesvalley.police.uk/advice/advice-and-information/asb/af/antisocial-behaviour/
- Simplify to bullying, graffiti, etc.

How to deal with anti-social behaviour

- Follow your organisation's policies and procedures
- Speak to the person
- Explain the situation and the risks of the anti-social behavior
- Explain the consequences if the anti-social behavior continues
- Remain calm
- Ensure that your colleagues know about the situation and that you have back-up if needed
- Remain vigilant.

296

Anti-social behaviour

Further ways in which to deal with anti-social behaviour are detailed on the next slide.

- Conduct high-profile patrols
- Promote early intervention
- Use positive, non-aggressive communication
- Promptly report incidents
- Accurately record incidents
- Liaise with police and other appropriate agencies.

Key Task 1

1 Identify FIVE factors that could make someone vulnerable.

1 ....

2 ....

3 ....

4 ....

5 ....

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

1 Identify FIVE factors that could make someone vulnerable.

1	Drink	**4**	Victim of domestic violence
2	Drugs	**5**	Young people (under 18).
3	Alone		

2 Identify behaviours that may be exhibited by sexual predators.

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

2 Identify behaviours that may be exhibited by sexual predators.

Close monitoring of vulnerable people e.g. someone looking lost or alone
Buying drinks for people who are already intoxicated.

This list is not exhaustive

Key Task 1

③ **Identify indicators of abuse.**

1 ....
2 ....
3 ....
4 ....

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

(3) Identify indicators of abuse.

1 Restricted freedoms of individuals

2 Unexplained bruising

3 Lack of confidence and insecurity

4 Change of personal circumstances.
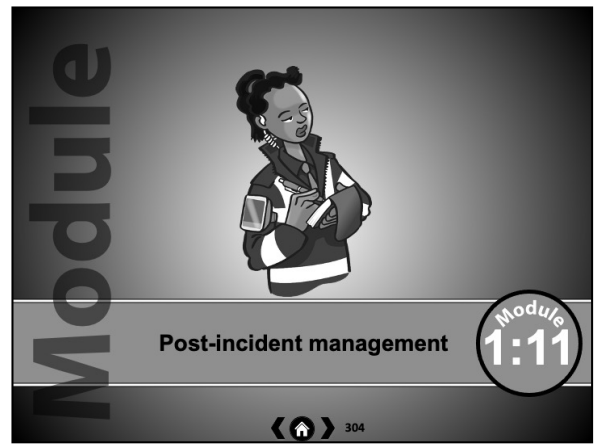
Post-incident management

Module 1:11

304

Completion of this module will enable learners to meet the following learning outcome:

Learning outcome 11: Understand good practice for post incident management

This includes assessment criteria:

11.1 Identify sources of post incident support available

11.2 State why accessing support following an incident is important

11.3 State the benefits of reflecting on incidents

11.4 Identify why it is important for security operatives to contribute to improving practice

This module includes the following interactive activities:

Key task 11

Anyone can be affected by something they have seen or experienced, for example:

- violence in the workplace
- a first-aid incident such as a heart attack or seizure
- a traffic accident
- serious injury from equipment
- a lost child.

No one is immune from shock or post-traumatic stress disorder (PTSD).

Most people will be affected at some point in their lives, whether the effects are temporary or long-term.

Experiencing stress or PTSD is not a sign of weakness.

Accessing help and support

It is important that businesses and organisations are able to help staff after an incident, particularly in relation to:

- providing immediate and ongoing support
- helping all members of staff to learn from the incident
- updating policies and procedures to improve safety
- sharing good practice.

306

Accessing help and support following conflict

Because of their varying degrees of experience and exposure to conflict, people cope with stress in different ways

Incidents where people are abused, threatened or even assaulted in the workplace can have various different impacts and so all security operatives need to be aware of what is available out there to help them if they need assistance or support following a traumatic incident.

Typical symptoms are how the brain and body react to abnormal situations or incidents

The severity of the symptoms can depend on the severity of the incident

In the time following the incident, anyone could start to feel shock, anger, embarrassment or disbelief.

Responses to incidents

Ensure that learners are aware that something that might not affect them could well affect one of their colleagues and vice versa.

Typical effects

Short-term and long-term symptoms following exposure to workplace violence could include:

- sickness
- insomnia
- behavioural changes
- becoming withdrawn
- anxiety
- intolerance
- hypersensitivity

- fear
- depression
- loss of confidence
- stress
- post-traumatic stress disorder (PTSD).

KEY POINT

It is vital that if a member of staff starts to show any signs that they may be suffering from any of these symptoms, support must be given immediately to reduce the changes of long term effects.

Support can be provided by:

- colleagues
- management
- counsellors
- helplines (such as the Samaritans)
- citizen's advice
- trade unions
- trade publications such as victim support

(www.victimsupport.org.uk/)

Professional medical help may even be required for serious problems.

MIND also have some very informative online guides for staff and managers.

Reflecting on and learning from conflict

The above is especially true when it comes to how people deal with conflict, anger, aggression and violence.

There are 6 basic steps to take following an incident of violence in the workplace.

STEP 1 Reflect on what happened

• Look for the good and bad in all cases.

2 STEP 2 – Recognise trends and any poor practice

Consider
- Does this problem occur regularly?
- At any particular place or time?
- Can you reduce or stop these types of incidents?
- Is there something you are doing wrong?
- What is the common response to this type of situation?

313

STEP 2   Recognise trends and any poor practice

- Are staffing levels sufficient?
- Has the footfall increased, is it seasonal, etc.?

3 STEP 3 – Share good practice

Consider
- Did you do something well?
- Does everyone know how to do it?
- Is extra training required?
- Does it need to be a policy?

314

STEP 3   Share good practice

- People often forget to accept praise for a job well done.

STEP 4   Learn from what happened

• Remember, there is such a thing as the 'bad shift'. Sometimes improvements cannot be made as the circumstance is highly unlikely to arise again.

STEP 5   Update policies, practices and procedures

6 STEP 6 – Monitor progress

Consider
- How can you record future incidents better?
- How can you monitor the effectiveness of any changes made?
- When and how can you re-evaluate your future performance?

317

STEP 6   Monitor progress

• Always consider the possibility of legal action being taken against the company. Due diligence may protect the contract and therefore jobs.
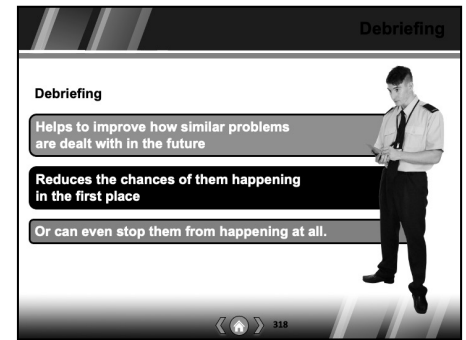
The proper debriefing of these types of incidents can help security operatives to improve how they deal with similar problems in the future.

Organisations can use data that has been collected for licensing hearings and they may even be able to reduce the chances of them happening in the first place or even stop them from happening at all.

If they do occur, security operatives should be able to provide an agreed, common positive response each time, automatically improving their own safety.

It is in everyone's best interest to be continually improving your work practices. Good debriefings and therefore reflection can:

- promote a professional service
- increase safety for staff
- promote teamwork
- increase safety for customers
- identify procedures or methods to better deal with situations effectively.

Like all industries, the security industry needs to continue to evolve and progress.

Security operatives have the responsibility to ensure that they continually contribute to improving practices within the industry.

① **Explain where post-incident support or resources can be found.**

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

1 **Explain where post-incident support or resources can be found.**

Colleagues, management, counsellors or helplines.

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

This list is not exhaustive.

② **Explain why it is important to access support following an incident.**

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

(2) **Explain why it is important to access support following an incident.**

People cope with assaults and incidents in different ways. Anyone can start to feel shock, anger, embarrassment and disbelief.

This list is not exhaustive.

3 **Identify indicators of abuse.**

1 .... **3** ....

2 .... **4** ....

.... **5** ....

Ask delegates to complete the key tasks for this section in their handouts, or to complete it in groups in the classroom.

3 Identify indicators of abuse.

1 Learn from what happened

2 Update policies, practices and procedures if required

3 Increase staff safety

4 Increase safety for customers

5 Promote teamwork.

1. to put into practice what you have learnt

2. to develop competency in your work activities

3. to keep your knowledge up to date

4. to pass the examination.

Thank you for listening

quality, value, service & integrity

Highfield
Products