Qualification Specification

Highfield Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry

Qualification Number: 603/5534/7

Version 1.6 October 2021

Highfield ICON, First Point, Balby Carr Bank, Doncaster, South Yorkshire, DN4 5JQ,
United Kingdom Tel +44 01302363277

Contents

Highfield Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry

Introduction

This qualification specification is designed to outline all you need to know to offer this qualification at your centre. If you have any further questions, please contact your account manager.

Qualification regulation and support

The **Highfield Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry** is awarded by Highfield Qualifications and sits on the Regulated Qualifications Framework (RQF). The RQF is a Qualification Framework regulated by Ofqual and CCEA Regulation. The qualification is also regulated by Qualifications Wales.

This qualification is supported by the Security Industry Authority (SIA), who regulate the private security industry.

Key facts

Qualification number:	603/5534/7
Learning aim reference:	60355347
Credit value:	3
Assessment method:	Multiple-choice examinations and practical demonstrations
Guided learning hours (GLH):	30
Minimum contact time (MCT):	22*
Total qualification time (TQT):	30

*** The SIA stipulates a minimum number of contact hours and a minimum number of training days. 22 hours applies as minimum contact time only where self-study can be evidenced. No self-study means a minimum of 30 hours. See Guidance on Delivery for details.**

Qualification overview and objective

The objective of this qualification is to support a role in the workplace. It is designed for learners wishing to apply for a licence from the Security Industry Authority (SIA) to work as a CCTV operator and is based on the relevant SIA specification for learning and qualifications.

Entry requirements

This qualification is approved for delivery to learners aged 16 and over. However, training centres must make it clear to those learners aged 16-17 that an SIA licence cannot be applied for until the age of 18.

Language prerequisite

Security operatives are likely in the course of their work to be required to make calls to the emergency services, or for example communicate to resolve conflict. It is essential that security operatives can communicate effectively.

It is the centre's responsibility to ensure that each learner is sufficiently competent in the use of the English and/or Welsh language. All initial language assessments must be conducted in the medium of English and/or Welsh as appropriate.

Learners should, as a minimum, have language skills in reading, writing, speaking, and listening equivalent to the following.

- A B2 Level qualification on the Home Office's list of recognised English tests and qualifications.
- A B2 Common European Framework of Reference for Languages (CEFR).
- An ESOL qualification at (Level 1) on the Ofqual register taken in England, Wales or Northern Ireland.
- An ESOL qualification at Scottish Credit and Qualifications Framework Level 5 awarded by the Scottish Qualifications Authority (SQA) and taken in Scotland.
- Functional Skills Level 1 in English.
- SQA Core Skills in Communication at Scottish Credit and Qualifications Framework Level 5.
- Essential Skills Wales Communication Level 1.
- Level 1 in Essential Skills – Communication Northern Ireland

Training centres must ensure that all learners have sufficient reading, writing, speaking and listening language skills before putting the learners forward for training and assessment.

All English/Welsh language assessments used by training centres must be agreed with their awarding organisation (AO) as part of their security approval.

Training centres must retain this information for all learners against all four competencies for a minimum of 3 years in line the with retention of assessment evidence requirements.

Geographical coverage

This qualification is suitable for learners in England, Northern Ireland and Wales.

Delivery/Assessment ratios

The ratio of trainers to learners is **1 trainer to a maximum of 12 learners** for the delivery and assessment of the practical skills.

When invigilating examinations, the maximum ratio is **1 invigilator to 30 learners**.

Centre requirements

To effectively deliver and assess this qualification, centres must meet the following:

Training and assessment of this qualification must be undertaken in a suitable training and assessment environment, which has been approved and quality assured by Highfield Qualifications. The environment must be adequately equipped for training, conducive to effective learning and must comply with current Health and Safety requirements. Equipment for practical activities must be readily available and fit for purpose.

For practical activities, the SIA considers it best practice to provide a realistic work environment for the training and assessment aspects of all practical activities stipulated.

Training and assessment facilities must comply with ongoing approval arrangements of Highfield Qualifications.

Centre Insurance

In line with general insurance requirements and the Employers Liability (Compulsory Insurance) Act 1969, the minimum for an approved centre offering licence-linked qualification is as follows:

- Employers Liability- £5 million
- Public Liability
- Professional Indemnity

Training centres are reminded of the importance of making sure their Public Liability and Professional Indemnity Insurance is set at the appropriate level whilst considering their business.

Examination Venue Criteria

Centres must adhere to the following when carrying out examinations.

- The seating arrangement for learners must ensure there can be no cheating or collusion between learners. All learners must be facing the same way (with the exception of some on-screen testing as detailed in bullet point 4).
- Each learner must be a minimum of 1.25 metres (centre to centre) each way from the next learner's workspace.
- Seating plans should be completed for the delivery of tests and retained for External Quality Assurance (EQA) purposes.
- If on-screen testing is being used each workstation must be isolated by a minimum space of 1.25 metres measured from the nearest outer edge of one screen to the next unless the monitors are positioned back-to-back. Under certain circumstances 1.25 metres may prove to be an insufficient distance to prevent learners from seeing, intentionally or otherwise, the work of others. Privacy screens can be used. The principal objective is to ensure that no Learner's work can be overseen by others.
- There must be a place for the invigilator to sit with a clear view of all learners.
- Maximum ratio is 1 invigilator to 30 learners.
- Walls must be clear of any material that would provide help to the learners.
- Examination signage and a clock must be in clear view of all learners.
- The awarding organisation must be made aware of assessment venues in advance. Only these can be used; not substitutes, unless there has been an emergency, such as a fire in which case this must be recorded, and the awarding organisation notified at the first possible opportunity in accordance with individual awarding organisation requirements.
- Trainers who have delivered the training and/or practical assessments to learners must not invigilate or be in the room when the learners take their exam for that subject(s). Training centres need to consider all potential conflicts of interest and have an appropriate policy in place to support this.
- All invigilators must receive an induction to the role of invigilation and its policies and procedures. Training centres must maintain a register which must be signed by the invigilator to confirm that they have received this induction.

- All test papers **must** be stored securely. Ideally, this should be a lockable safe. If a safe is not available a suitable lockable cabinet/storage unit will suffice. This unit should only be accessed by appropriate personnel and records of key holders should be kept. This cabinet/storage unit must be kept in a secure location.
- All test papers must be transported securely to and from the training centre and any satellite centre where tests are administered. The centre must have an appropriate policy to support this.
- Highfield Qualifications, the SIA and qualification regulators retain the right to make spot checks on examination days to ensure that exam conditions are being maintained.

Additional Requirements for the delivery of Principles and Practices of working as a CCTV operator in the private security industry

To be able to deliver and assess the learning outcomes and assessment criteria of unit Principles and Practices of Working as a CCTV Operator in the Private Security Industry, training centres must ensure:

- at a minimum, a CCTV system should have at least two PTZ cameras and associated recording and monitoring equipment within a control room. If a control room is not available a simulated control room environment must be used
- a simulated control room environment is a room that during training and assessment can be used solely for this purpose
- the ratio of trainers to learners; one trainer to a maximum of 12 learners for the delivery of practical skills with the assessment completed on a 1 – 1 basis
- the completion of documentation and portfolio creation can be conducted within a classroom (group) environment
- these practical assessments must take place after the delivery of the following units:
  - Principles of Working in the Private Security Industry
  - Principles and Practices of Working as a CCTV Operator in the Private Security Industry

Guidance on delivery

The total qualification time (TQT) for this qualification is **30 hours**, all of which are guided learning hours (GLH).

Please note 22 hours is the minimum contact time (MCT) as stipulated by the SIA which is applicable if self-study is applied to the Principles of working in the private security industry unit. If self-study isn't applied for this unit, then the MCT for this qualification will be 30 hours.

TQT is an estimate of the total number of hours it would take an average learner to achieve and demonstrate the necessary level of attainment to be awarded with a qualification, both under direct supervision (forming guided learning hours) and without supervision (all other time). TQT values are advisory and assigned to a qualification as guidance.

This section of the specification provides information on the specific delivery requirements of the qualification.

Minimum contact time (stipulated by the SIA)

The following table outlines the minimum contact time for each of the units contained within the Highfield Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry.

Minimum contact time is defined as the time that a learner must spend under the immediate guidance or supervision of a trainer, assessor or invigilator (including assessment). It does not include time spent checking ID or assessing English language skills, or breaks. This time will be monitored and **enforced** by Highfield Qualifications.

Unit No.	Unit reference	Unit title	Minimum Contact Time	GLH
1	J/617/9686	Principles of working in the private security industry	9*/17	17
2	R/617/9691	Principles and Practices of Working as a CCTV Operator in the Private Security Industry	13	13

*The SIA recognises that there is some learning that contributes to the achievement of the licence-linked qualifications that can be completed through self-study., as long as this is maintained with some form of support. It is therefore a requirement for centres wishing to use self-study to notify Highfield in advance and provide the details of how they intend to support learners and evidence this self-study. **The principles of working in the private security industry has a GLH of 17 hours, however, 8 of which can be delivered through self-study. The remaining 9 hours must be minimum contact time. If self-study isn't applied, then the MCT for this unit is 17 hours.**

The centre must detail within their quality management processes each of the following.

- The areas of learning delivered by self-study
- The method of self-study to be used
- The number of hours to be covered by the self-study material
- A robust and auditable method for determining that learners have undertaken the self-study

It is important the materials used clearly show learners, how many hours of learning they are expected to undertake and that they are given sufficient time to allow them to complete it before their course begins. It is also a requirement that the centre checks these during training to ensure appropriate learning has occurred. This will be quality assured through Highfield's external quality assurance processes.

Suitable methods of self-study resources include prepared, high-quality:

- online learning materials or courses that the learner must navigate
- workbooks that the learner must work through and complete
- learning materials that the learner can use to cover specific areas of content

Self-study may be used to deliver up to eight hours of Principles of Working in the Private Security Industry as follows:

Learning outcome	Content	Hours
1	Know the main characteristics and purposes of the private security industry	2
2	Understand legislation as it applies to a security operative	2
4	Understand the importance of safe working practices	2
5	Understand fire procedures in the workplace	1
11	Understand good practice for post-incident management	1

Centres are reminded that any self-study material used must be retained for a minimum of 3 years in line with the retention of assessment evidence requirements.

In addition to the above, if self-study is used, the SIA has stated that the training, delivery and assessment of this qualification must take place over a **minimum** of **3 days** (22 hours) and each day of training, delivery and assessment **must not** exceed **8 hours.**

If self-study is **not** used for this qualification, then the course **must** be delivered over **4 days** (30 hours) and each day of training, delivery and assessment **must not** exceed **8 hours.**

Centres must retain detailed registers that include start/end/break times of training for each day and these must be signed daily by the learners. This includes a record of any late arrivals/early leavers and how these learners made up the required hours which they missed. These must be retained for audit purposes. **Training centres must retain this information for a minimum of 3 years in line with the retention of assessment evidence requirements.**

Virtual learning delivery guidance

Virtual learning is an online platform that enables synchronous learning (live) and interactive delivery of training. This learning environment means that the tutors and learners can communicate (sound and visual) and interact with each other in an online group setting. Virtual learning may also be referred to as 'remote delivery training' or 'online classroom'.

Please note: Centres wishing to deliver using virtual learning must first be approved to do so. For further information on the approval process and requirements, centres should contact their account manager.

The tables below indicate which learning outcomes and assessment criteria can or cannot be delivered through virtual learning:

1. Principles of Working in the Private Security Industry	Virtual Delivery Acceptable	
Learning outcome	**Yes**	**No**
1. Know the main characteristics and purposes of the Private Security Industry*	All ACs	
2. Understand legislation as it applies to a security operative*	All ACs	

3. Understand arrest procedures relevant to security operatives	All ACs	
4. Understand the importance of safe working practices*	All ACs	
5. Understand fire procedures in the workplace*	All ACs	
6. Understand emergencies and the importance of emergency procedures	All ACs	
7. Understand how to communicate effectively as a security operative	All ACs	
8. Understand record keeping relevant to the role of the security operative	All other ACs	8.4 Demonstrate the accurate completion of an evidential statement (Section 9 Statement)
9. Understand terror threats and the role of the security operative in the event of a threat	All ACs	
10. Understand how to keep vulnerable people safe	All ACs	
11. Understand good practice for post incident management*	All ACs	

*Designates content that can also be taught through self-study.

2. Principles and Practices of Working as a CCTV Operator in the Private Security Industry	**Virtual Delivery Acceptable**	
Learning outcome	**Yes**	**No**
1. Understand the purpose of a surveillance (CCTV) systems and the roles and responsibilities of control room team and other stakeholders	All ACs	
2. Understand the different types of legislation and how they impact on Public Space Surveillance (CCTV) operations	All ACs	
3. Understand the importance of operational procedures in public space surveillance (CCTV) operations	All ACs	
4. Understand how public space surveillance (CCTV) systems equipment operates	All ACs	
5. Understand Surveillance techniques	All ACs	
6. Understand different types of incidents and how to respond to them	All ACs	
7. Understand health and safety in the CCTV environment	All ACs	

8. Demonstrate operational use of CCTV equipment		All ACs
9. Produce evidential documentation		All ACs

Additional unit delivery requirements:
Learners undertaking this qualification must be trained in the following **before** they undertake the one-to-one CCTV practical assessment:

- Principles of Working in the Private Security Industry
- Principles and Practices of working as a CCTV Operator in the Private Security Industry

Guidance on assessment

This qualification is graded as pass/fail.

This section of the specification provides information on how the qualification's individual components are assessed, along with any further specific requirements:

Unit No.	Unit reference	Unit title	Knowledge assessment method	Practical assessment method
1	J/617/9686	Principles of working in the private security industry	Externally set and marked multiple-choice question (MCQ) examination made up of 72 questions (110 minutes) Pass mark = 70%	Externally set, internally assessed activity based on the completion of an evidential statement Pass mark = 100%
2	R/617/9691	Principles and Practices of Working as a CCTV Operator in the Private Security Industry	Externally set and marked MCQ exam made up of 40 questions (60 minutes) Pass mark = 70%	Externally set and internally assessed practical CCTV scenario with portfolio and observation sheet Pass mark – 100% And Externally set and internally assessed workbook Pass mark = 80% for the short answer element of workbook **The practical assessment for each learner must be**

				visually recorded† and is recommended to take approximately 25 minutes per learner.

Each learner MUST be assessed individually when undertaking the practical demonstrations.

Following the assessments, all knowledge paperwork and assessment packs must be returned to Highfield. Upon successful processing, a list of results will be provided to the centre contact stating whether learners have passed or failed, along with certificates for those learners that have met the required standard.

All knowledge and written practical assessment evidence must be retained by all centres for a minimum of 3 years for audit purposes. All practical assessments must be video recorded and retained by all centres for a minimum of 1 year for audit purposes.

All internal assessments must be internally quality assured and are subject to external quality assurance.

†Those aged 16 and 17 are exempt from the requirement to visually record their practical assessment. In these cases, training centres must provide alternative evidence, such as a transcript. Training centres must make clear to them that they cannot hold a licence until the age of 18.

Centres must take all reasonable steps to avoid any part of the assessment of a learner (including any internal quality assurance and invigilation) being undertaken by any person who has a personal interest in the result of the assessment.

Please note: tutors/assessors who have delivered the training and/or practical assessments to learners must not invigilate or be in the room when the learners take their exam for that subject(s). Centres need to consider all potential conflicts of interest and have an appropriate policy in place to support this.

Guidance on quality assurance

To support with quality assurance, Highfield require centres to undergo a security approval visit prior to the delivery of the qualification. Upon successful completion of this, centres are then permitted to register and deliver courses. This security approval is revisited on at least an annual basis.

In addition to the regular monitoring/support visits, Highfield recommends that centres have a quality assurance system in place prior to the return of assessment material to Highfield for external assessment/moderation. This is to ensure assessments are of the highest standard for every course.

Highfield Qualifications requires centres to have in place a robust mechanism for internal quality assurance. Internal quality assurance must be completed by an appropriately qualified person and that person must not have been involved in any aspect of the delivery or assessment of the course they are quality assuring. **For further guidance on IQA processes, please refer to the tutor, assessor and IQA (TAI) support pack for this qualification, found in the Download Area of the Highfield Qualifications website.**

Recognition of prior learning (RPL)

Where a unit is contained within several Highfield qualifications, learners can transfer the achievement of this unit:

The **Principles of working in the private security industry** unit is contained in the following Highfield qualifications:

- Highfield Level 2 Award for Door Supervisors in the Private Security Industry
- Highfield Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry
- Highfield Level 2 Award for Security Officers in the Private Security Industry

Learners cannot transfer unit achievement from previous security qualifications (those available before April 2021) to this qualification.

Tutor/assessor requirements

It is expected that in most cases the tutor and the assessor will be the same person.

To deliver this qualification (and the units contained within it) tutors/assessors are required to hold the following:

Training qualification

Tutors are required to hold a teaching or training qualification at Level 3 or above, which has been accredited by SQA/QCA/Ofqual or validated by an HEI, or an equivalent such as:

- Level 3 Award in Education and Training or equivalent
- Level 4 Certification in Education and Training or equivalent
- Certificate in Education
- Postgraduate Certificate in Education
- SVQ/NVQ Levels 3 and 4 in Learning and Development
- Scottish Training Qualification for Further Education (TQFE)
- Masters in Education

NaCTSO counterterrorism programme

Tutors must also successfully complete a National Counter Terrorism Security Office (NaCTSO)/SIA-endorsed counterterrorism programme such as the ACT (Action Counters Terrorism) Awareness training and the ACT security e-learning module, both of which **must** be completed annually.

Assessor qualification

Assessors **must** hold one of the qualifications below. If they don't hold one of these qualifications currently, they **must** achieve one of the qualifications below by **30 September 2022**:

Assessors to hold any of the following qualifications:

- Level 3 Award in Understanding the Principles and Practices of Assessment (RQF)
- Level 3 Award in Assessing Competence in the Work Environment (RQF)
- Level 3 Award in Assessing Vocationally Related Achievement (RQF)
- A1 Assessing Learners Using a Range of Methods
- D32 Assess Learner Performance
- D33 Assess Learner Using Different sources of Evidence

Or the following unit from an assessor qualification.

- Unit 1 Understanding the principles and practices of assessment

Or the following units from a teaching qualification.

- Understanding assessment in education and training unit (from a Level 3 Award in Education and Training)
- Understand the principles and practices of assessment (from a 12 credit Preparing to Teach in the Lifelong Learning Sector)
- Principles of assessment in lifelong learning (from a 12 credit Preparing to Teach in the Lifelong Learning Sector)
- Understanding the principles and practices of assessment (from a Level 3 Certificate/Level 4 Diploma in Learning and Development)
- Assess occupational competence in the work environment (from a Level 3 Certificate/Level 4 Diploma in Learning and Development)
- Assess vocational skills, knowledge and understanding (Level 3 Certificate/Level 4 Diploma in Learning and Development)

Sector competence

Tutors/assessors delivering the learning leading to licence-linked qualifications must demonstrate that they have the necessary experience, knowledge and understanding of the sector in which they are providing training.

To demonstrate this, Highfield will require sufficient information about a tutor/assessor's occupational experience for consideration in the approval process, for example, experience of working in the private security industry or working in a role that can be mapped to the requirements of the private security industry. There is no requirement for a tutor/assessor to have a current SIA licence.

Other relevant experience could come from employment* in:

- armed services
- police service
- security industry
- prison service

*With appropriate front-line experience being mapped into the desired qualification or unit.

To ensure that tutors have the right occupational expertise, the SIA require that:

- tutors new to the sector (i.e. this is their first role as a trainer/assessor in the security sector as identified by their CV) have a minimum of **2 years'** frontline operational experience **in the last 5 years**, which is relevant to the qualifications that they are delivering. This experience should have been gained in the UK. This operational experience can be achieved from full/part-time/weekend employment and achieved in blocks of employment if it meets the threshold above.
- existing tutors/assessors must be able to demonstrate evidence of a suitable level of continued professional development (CPD) in their sector. This should include the equivalent of at least 40 hours every year spent in a combination of training, increasing professional knowledge through other means, or working in the industry. Suitable steps could include attendance at relevant conferences and seminars and continuing work experience in the sector. This CPD record must show that a National Counter Terrorism Security Office (NaCTSO)/SIA-endorsed counter

terrorism programme such as the ACT (Action Counters Terrorism) awareness training has been completed on an annual basis.

It is the responsibility of training centres to retain the CPD information of trainers and assessors. Highfield and the SIA reserve the right to spot check this information for accuracy and quality assurance (QA) purposes. **This evidence must be retained for a minimum of 3 years for audit purposes.**

The SIA may publish additional requirements for tutor/assessors as and when they are agreed. Tutors looking to deliver licence-linked qualifications should ensure that they are fully familiar and compliant with the requirements detailed within the qualification.

Tutors/assessors who are unsure about their current qualifications or who wish to check their eligibility should contact their Highfield account manager.

Internal quality assurance (IQA) requirements

Internal quality assurers (IQAs) **must** hold one of the qualifications below. If they don't hold one of these qualifications currently, they must achieve one of the qualifications below by 30th September 2022.

Internal quality assurer (IQA) to hold any of the following qualifications:

- Level 4 Award in Understanding the Internal Quality Assurance of Assessment Processes and Practices (RQF)
- Level 4 Award in the Internal Quality Assurance of Assessment Processes and Practices (RQF)
- Level 4 Certificate in Leading the Internal Quality Assurance of Assessment Process and Practices (RQF)
- V1 Conduct Internal Quality Assurance of the Assessment Process
- D34 Internally Verify the Assessment Process

Or the following unit from an IQA qualification:

- Unit 2/Unit 4 Understanding the principles and practices of internally assuring the quality of assessment.

Highfield will require sufficient information about the occupational competence of an IQA which will be considered by the Highfield on a case-by-case basis.

Reasonable adjustments and special considerations

Highfield Qualifications has measures in place for learners who require additional support. Please refer to Highfield Qualifications' Reasonable Adjustments Policy for further information/guidance.

ID requirements

It is the responsibility of each centre to have systems in place to ensure that the person taking licence-linked qualifications is indeed the person they are purporting to be.

All centres are therefore required to ensure that each learner's photograph and formal identification documents are checked and recorded before they are allowed to sit the examination/assessment.

When completing the ID validation sheet, all photographs supplied by the learners must be checked to ensure each one is a true representation of the individual. Once satisfied, they must print the learner's name on the reverse of the photograph before sticking it onto the adhesive film on the identification validation sheet.

A list of current documentation that is accepted by the SIA as proof of identification is available on the SIA website here.

Any learner who does not produce the required documents to satisfy the ID requirements cannot take any assessments and therefore will not be able to complete the qualification. Anyone in this situation should contact the SIA directly via their online account to:

- explain why they do not possess the required documents
- tell the SIA what documents they do have

The SIA will then assess this evidence on a case-by-case basis.

Progression opportunities

Progression and further learning routes could include:

- Highfield Level 2 Award for Security Officers in the Private Security Industry
- Highfield Level 2 Award for Door Supervisors in the Private Security Industry
- Highfield Level 3 Certificate for Working as a Close Protection Operative within the Private Security Industry
- Highfield Level 3 Award in the Delivery of Conflict Management Training (RQF)
- Highfield Level 3 Award for Physical Intervention Trainers in the Private Security Industry

Useful websites

- British Security Industry Authority http://www.bsia.co.uk/
- Home Office http://www.homeoffice.gov.uk/
- SIA http://www.sia.homeoffice.gov.uk/Pages/home.aspx
- The Information Commissioner http://ico.org.uk
- NaCTSO https://www.gov.uk/government/organisations/national-counter-terrorism-security-office

Recommended training materials

Working as a CCTV Operator Course Book. Walker, A. and Porter, S. Highfield.co.uk Ltd

Appendix 1: Qualification structure

To complete the **Highfield Level 2 Award for CCTV Operators (Public Space Surveillance) in the Private Security Industry**, learners must complete **all units** contained within the following mandatory group.

Unit reference	Unit title	Level	GLH	Credit
J/617/9686	Principles of working in the private security industry	2	17	2
R/617/9691	Principles and Practices of Working as a CCTV Operator in the Private Security Industry	2	13	1

Important note:
There are **no** RPL opportunities for old units (linked with historic security qualifications) that will allow for certification of the above qualification. Therefore, all units linked to this qualification must be completed in full for a learner to be awarded.

Appendix 2: Qualification content

Unit 1: **Principles of working in the private security industry**
Unit number: J/617/9686
Credit: 2
Min. contact time: **9 (If self-study is applied. If self-study isn't used, then the MCT is 17 hours)**
GLH: 17
Level: 2

Learning Outcomes	Assessment Criteria
The learner will	***The learner can***
1. Know the main characteristics and purposes of the private security industry	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
2. Understand legislation as it applies to a security operative	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
3. Understand arrest procedures relevant to security operatives	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

Learning Outcomes	Assessment Criteria
The learner will	*The learner can*
4. Understand the importance of safe working practices	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
5. Understand fire procedures in the workplace	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 firefighting equipment 5.6 Identify the role of a fire marshal in the event of an emergency
6. Understand emergencies and the importance of emergency procedures	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
7. Understand how to communicate effectively as a security operative	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
8. Understand record-keeping relevant to the role of the security operative	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

Learning Outcomes	Assessment Criteria
The learner will	***The learner can***
9. Understand terror threats and the role of the security operative in the event of a threat	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
10. Understand how to keep vulnerable people safe	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
11. Understand good practice for post-incident management	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 incident 11.4 Identify why it is important for security operatives to contribute to improving practice

Assessment Guidance

Please find guidance below regarding the practical assessments associated with this unit. All practical assessment templates are available from the Download Area of the Highfield Qualifications website.

- **AC 8.4: Demonstrate the accurate completion of an evidential statement (Section 9 Statement)**

Learners are required to produce a **hand-written** statement, based on a scenario provided by the centre using the evidential statement template provided. In order to achieve the criteria, reports **must** include these key areas:

- The author of the report **(I am)**
- The date of the report **(On)**
- Where the incident happened (**At)**
- The time of the incident (**About**)
- What they saw/did (**I was/I saw/I did)**
- Signature of the report author

An example scenario (attempted theft) and an exemplar statement are available within the Tutor, Assessor and IQA (TAI) support pack found in the Download Area.

Indicative Content

LO1 Know the main characteristics and purposes of the private security industry

1.1 Identify the key purposes of the private security industry
- Prevent and detect crime and unauthorised activities
- Prevent and reduce loss, waste and damage
- Monitor and respond to safety risks
- Provide personnel and appropriate protection systems for people, property and premises
- Raise standards in the industry

1.2 State the aims and functions of the Security Industry Authority (SIA)
- Protect the public and regulate the security industry through licensing
- Raise standards (through the Approved Contractor Scheme)
- 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

1.3 Recognise the required standards of behaviour of a security operative
- Main qualities required for security industry operatives: reliability and integrity; politeness; professional attitude and appropriate personal appearance; being prepared to take responsibility
- Skills: communication skills, observational skills, problem solving, ability to handle sensitive situations, team-working skills
- Adherence to SIA Standards; adherence to organisation/company values and standards

1.4 Identify the benefits of community safety initiatives
- Examples of community safety initiatives: police liaison officers, police community links, initiatives to radio link with other venues e.g. National Pubwatch, local Pubwatch initiatives, sharing information, red and yellow cards
- Aim: to reduce the opportunity for crime to take place
- Activities: include improving physical security of vulnerable targets, improving the environment, removing the means to commit crime; improving the visibility in an area e.g. lighting; controlling access to areas so unauthorised people cannot gain access to commit crime; initiatives to radio link with other venues e.g. National Pubwatch, local Pubwatch initiatives, sharing information, red and yellow cards
- Benefits: include better partnership working, cooperating with Local Authority and police, liaison with other venues, reduction of risk of crime to own employer or other employers, promotion of safer communities

1.5 Recognise how assignment instructions support the security operative role
- Describes the security operative's roles and duties for specific location
- Outlines actions to take in an emergency including obtaining contact numbers

- Part of a contract between client/customer and the security company

1.6 Recognise how each security operative role may use CCTV
- Benefits of using CCTV e.g.:
  - prevents crime
  - cuts down on incidents
  - reduces costs by not having to employ additional staff
  - can provide clear evidence for investigations
  - can provide evidence that can be used in a court of law
- Understand the legal implications of using CCTV e.g.:
  - must be registered
  - must have a named person who is responsible and accountable for its use
  - must display signs to inform people that CCTV is in operation
  - must not record in private spaces such as toilets
- Must comply with current data protection legislation e.g.:
  - when storing data including any recordings
  - restricting access to certain staff
  - by using recordings appropriately

1.7 Identify the limitations of CCTV within the security operative role
- Privacy issues and concerns
- Vulnerable to damage and vandalism
- Misuse
- Cannot prevent crime
- Cost
- Familiarity with scope of cover
- Technology vulnerabilities

1.8 State the purpose of the Approved Contractor Scheme
- Raise performance standards
- Assist the SIA to develop new opportunities
- Increased customer confidence

LO2 Understand legislation as it applies to a security operative

2.1 Identify the differences between civil and criminal law
- Main features of civil law:
  - purpose to right a wrong
  - individual brings the cases
  - remedy by compensation for loss or damage
  - standard of proof on balance of probabilities
- Examples of civil offences:
  - libel
  - slander
  - breach of contract
  - employment law
  - family and matrimonial disputes
  - property disputes
  - personal injury cases
  - trespass

- Main features of criminal law:
  - purpose to deter and punish
  - state brings the cases
  - remedy is fines/imprisonment
  - standard of proof is beyond reasonable doubt
- Examples of criminal offences:
  - driving under the influence
  - assault
  - murder
  - rape
  - child abuse
  - theft
  - domestic abuse
  - arson
  - kidnapping or holding someone against their will

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

- Raise standards in the private security industry
- Increase public confidence in the private security industry
- Increase public safety
- Remove criminal elements from the private security industry
- Established the SIA (Security Industry Authority)
- Established licensing

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

- Key Legislation - Equality Act 2010 (not Northern Ireland – see NI specific information below); Human Rights Act 1998
- Protection from discrimination in the workplace:
  - protected characteristics - race/ethnicity/nationality, gender, religion or belief, disability, sexual orientation, gender reassignment, marriage/civil partnership, age, pregnancy and maternity
  - direct and indirect discrimination
- Areas where equal opportunities legislation applies:
  - Recruitment, access to training, pay and benefits, promotion opportunities, terms and conditions, redundancy, dismissal
- Employer's duty to make reasonable adjustments

For Northern Ireland

- Discrimination is illegal
- A security operative cannot refuse entry or evict anyone on the grounds of sex, race, colour, disability or physical appearance.
- The following laws relate to discrimination:
  - The Race Relations (Northern Ireland) Order 1997
  - The Sex Discrimination (Northern Ireland) Order 1976
  - The Disability Discrimination (Northern Ireland) Order 2006.
- Should a security operative refuse entry to, or evict an individual for any of these reasons alone then they commit 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 again you and your employer.

2.4 Identify licensable roles under the Private Security Act
- Licensable roles
- Licensed sectors in:
  - manned guarding, vehicle immobilisation, security guarding, door supervision, CCTV, close protection, cash and valuables in transit (CVIT), key holding

2.5 Identify how data protection regulation impacts on the security operative
- Have an understanding of current data protection regulation, including the general principles
- The use of body-worn cameras and restrictions, e.g.:
  - images must be stored to comply with GDPR and can only be viewed by authorised personnel
- Recording and documenting in notebooks

LO3 Understand arrest procedures relevant to security operatives

3.1 State the meaning of arrest
- Arrest is to take away someone's liberty
- There is no legal definition for citizen's arrest
- Police and non-police arrest
- Arrest with a warrant
- Arrest without a warrant

3.2 Identify offences for which a security operative can make an arrest
- Security operatives have no special powers of arrest, only the same powers of arrest as every other citizen.
- Arrestable offences, indictable offences and breach of the peace
- Indictable offences are usually tried at the Crown Court
- Powers of arrest under the common law
- Offences include:
  - murder/homicide
  - aggravated assault
  - assault
  - rape
  - sexual assault
  - firearms offences
  - robbery
  - burglary
  - theft
  - drugs offences
  - fraud
  - criminal damage

3.3 Identify the limitations to a security operative's powers of arrest
- Must be within powers of citizen's arrest
- Section 24a of the Police and Criminal Evidence Act 1984, S26a of the Police and Criminal Evidence (Northern Ireland) Order 1989 (SI 1989/1341)

- Indictable offence must be either being committed or have already been committed
- Arrest can only be made to prevent the person from:
  - causing injury to himself or another
  - suffering injury himself
  - causing loss of or damage to property
  - making off before a constable can assume responsibility for him

3.4 State procedures to follow when making an arrest

- Inform person that they are under arrest, provide the reason for arrest, and that the police will be called
- Detain the person and ensure their safety
- Use witnesses wherever possible
- Only use reasonable and necessary force to prevent:
  - escape of individual under arrest or assault against security operatives or others

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

- Taking someone's liberty is a serious matter
- Can only arrest for indictable offences
- False arrest can lead to civil or criminal prosecution of the security operative making the arrest
- Personal safety of the security operative can be at risk

3.6 State procedures following an arrest

- The arrested person is now the security operative's responsibility
- Ensure own safety
- Ensure the person's safety
- Ensure any evidence is preserved and not disposed of
- Hand person over to police, explaining reason for arrest
- Inform police of any extra evidence of offence (witnesses, CCTV, property)
- Record arrest in line with local policy
- Assist police with a statement if required
- Attend court at a later date if required
- Identify how to work with the police in relation to arrest procedures

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

- Reasonable force is the amount of force that can be used to protect yourself or your property from attack. It can be used to prevent crime or when detaining someone through a citizen's arrest. It can also be classed as 'legal force'
- Necessary force is an opinion of the level of force that was carried out in any situation

LO4 Understand the importance of safe working practices

4.1 Identify responsibilities under the Health and Safety at work etc. Act/The Health and Safety at Work (Northern Ireland) Order 1978)

- Responsibilities of employees and the self-employed
  - to take responsibility for own health and safety
  - to cooperate with employer
  - to take reasonable care and not put themselves or public at risk
  - to report injuries and accidents to employer
  - to follow instruction, processes and procedures put in place by their employer

- Responsibilities of employer
  - to maintain the safety of employees and anyone who visits the premises
  - to provide safe access and egress
  - to assess and reduce risk, to provide first-aid facilities, to tell staff about hazards, to provide training if required, to record injuries and accidents, to provide and maintain necessary equipment and clothing and warning signs
  - to comply with legislation - consequences of failure to comply e.g. prosecution, business closure

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

- Being isolated and having to rely on technology for back-up
- Being vulnerable:
  - injury/ill health
  - violence
  - lack of support
  - lack of communication
  - lack of welfare facilities for rest

4.3 Identify typical workplace hazards and risks

- Definition of hazard:
  - potential source of harm or adverse health effect on a person or persons
- Typical workplace hazards:
  - accidents due to poor lighting, uneven surfaces, steps, etc.
  - risk of infection from body fluids
  - risk of dealing with aggressive or violent behaviour
  - injuries from poor manual handling
  - misuse/abuse of machinery
  - sharp objects (needles and knives)
  - diseases
  - hazardous chemicals
  - noise pollution
  - moving vehicles
  - obstructions
  - poor lighting
  - fire/floods and other emergencies
- Definition of 'risks':
  - likelihood that a person may be harmed or suffer adverse health effects if exposed to a hazard
- Identify typical risks:
  - level of risk (high, medium or low impact)
  - assess the risk of the hazard by identifying who may be harmed and how, what controls are already in place, what additional controls are needed to control the risk, who is required to do this and when is it required to be completed by

4.4 State how to minimise risk to personal safety at work

- Risk assessment - developing awareness of risks and how to minimise them
- Following health and safety and organisational procedures in relation to health and safety
- Use of protective equipment, personal alarms and mobile phones
- Importance of following safe routines and being systematic

- Identify methods for safe manual handling
  - assessment of load, know own limits, plan route; use of mechanical aid, stable base, correct positioning of head, feet and back, correct positioning of load, smooth movements, avoidance of twisting, push rather than pull
- Follow health and safety and organisational procedures in relation to global (or critical) incidents

4.5 Identify safety signs and signals

- Different categories of sign, e.g.:
  - prohibition, warning, mandatory, safe condition, firefighting, hazard/chemical warning plates

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

- RIDDOR - Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013/ Northern Ireland - RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (Northern Ireland) 1997
- Reportable incidents and accidents under RIDDOR: work-related, dangerous occurrence, resulting in injury, occupational disease or death; gas-related incident
- Procedures: in line with organisational procedures; record in accident book; RIDDOR reporting – 'responsible person', online, telephone, by post
- Remember to include who, what, when, how and where

4.7 Identify ways to keep personal information safe

- When handling any personal information or data (either their own or someone else's) security operatives must:
  - comply with current data protection legislation
  - follow organisational procedures
  - follow assignment instructions
  - maintain confidentiality of information
- Security operatives should:
  - use personal social media responsibility including managing privacy settings
  - not wear anything identifiable outside the workplace
  - keep personal vigilance e.g. not completing surveys
  - not discuss work issues outside the workplace
  - not discuss work information with colleagues

LO5 Understand fire procedures in the workplace

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

- Components of fire: the fire triangle (oxygen, fuel, heat - chemical chain reaction)

5.2 State the actions to be taken upon discovering a fire

- Follow organisation's policies and procedures
- Sound the alarm and inform emergency services
- FIRE (Find, Inform, Restrict, Evacuate or Extinguish) - do not attempt to put out a fire if it puts you in danger.
- Identify area where fire is, isolate other areas

- Control panel - important to ensure full understanding of extent of area of incident, to pass on correct message to emergency services e.g. with regard to materials, chemicals stored in affected area

5.3 Identify basic fire safety controls

- Be observant and vigilant
- Control of fuel and ignition sources e.g. bins and waste disposal
- Safe storage of flammables
- Inspection and maintenance of electrical equipment
- Avoidance of overloading electrical points
- Follow staff training
- Adhere to fire plan

5.4 Identify classifications of fire

- A – Ordinary combustible: including paper, wood, textiles, rubber
- B – Flammable liquids e.g. petrol, paint, solvents
- C – Flammable gas e.g. butane, propane
- D – Metal fires e.g. powdered and metal shavings, alkali-based metals
- Electrical fires (no classification as electricity is a source of ignition as opposed to a fuel).
- F – Hot cooking oils

5.5 Identify the different types of fire-fighting equipment

- Extinguishers:
  - water for use with paper, wood
  - general foam for use with paper, wood/ specialist foam for use with industrial alcohol
  - CO^2 Gas for use with electrical fires (primary)/flammable liquids (secondary)
  - wet Chemical, for cooking oil fires
  - powder for use with most fires including liquid and electrical fires
- Other equipment:
  - fire blankets, fire hose, sprinkler system

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

- Sound the alarm
- Check allocated area to ensure that everybody has left, take roll call
- Take control of the evacuation and ensure that anybody with evacuation difficulties is aided
- Proceed to the assembly area and report to the fire officer in charge

LO6 Understand emergencies and the importance of emergency procedures

6.1 Identify the key emergency terms

- An emergency is a situation that is unexpected, threatens safety or causes serious disruption and requires immediate action
- Emergencies can include incidents, occurrences, accidents, examples are listed below:
  - Incident/Occurrence – this could include a fight, power cut or drug overdose, etc.
  - Emergency – this could include health emergencies such as epileptic seizure, anaphylactic shock, heart attack, etc.
  - Accident – this could include someone falling down steps, someone slipping on a wet floor, etc.

6.2 Identify different types of emergencies within the workplace

- Types of emergency:
  - power, system or equipment failure; flood; actual or threatened serious injury; serious illness; bomb threat, fire, terror threat

6.3 Recognise how people react when emergencies occur

- Types of reactions:
- Public/Human responses – fight or flight
- Panic, freeze
- Crowd control, danger of crushing

6.4 Identify actions to be taken in an emergency situation

- Security operative responses to emergencies:
  - follow correct procedures depending on emergency
  - ensure safety of self and others
  - report to appropriate authorities
  - act quickly, be authoritative, remain calm, encourage others to remain calm
  - follow procedures for making emergency calls
  - follow escalation procedures if required
  - document clearly what happened and your response
  - review and evaluate incident
  - identify how a graduated response can be applied to incidents

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

- List actions to be taken when first aid is required
- If necessary, contact designated first-aider or the emergency services
- Know the limits of your own ability and authority to deal with personal injury
- Record the injury in the accident book
- Keep people safe, including onlookers
- Provide privacy whenever possible

6.6 Recognise evacuation principles

- Evacuation – this is a controlled process of emptying an area or premises of people. Evacuation can be to an adjoining area within a building or outside depending on the severity of the incident. Examples for evacuation could be flood, fire or terror threat.
- Invacuation – this is a controlled process of getting people into safe premises due to an incident that could cause harm to people who were outside. For example, if a person with a firearm started to shoot people in the street you would encourage everyone into the building and lock the doors for safety.
- Basic principles are to keep people safe and to follow the organisation's policies and procedures.
- Importance of knowing venue specific requirements

LO7 Understand how to communicate effectively as a security operative

7.1 Identify the different types of communication

- Non-verbal communication - gesture, stance, eye contact, facial expression,
- Verbal communication - speaking, listening, reading, pitch, tone of voice
- Written communication - pictures, signs, script, text messages

7.2 State the importance of effective communication
- to ensure that the message being sent is received and understood by the recipient
- Features of effective communication include choosing language and medium appropriate for message and recipient, delivering message clearly, checking understanding
- Promotes effective teamwork
- Promotes a professional establishment and service
- Prevents misinterpretation which could lead to aggressive behaviour
- Prevents misunderstanding which could lead to mistakes
- Importance of effective communication: to ensure organisational effectiveness and effective team working, to provide effective service to customers
- NATO phonetic alphabet: Call signs: correlate to each letter from phonetic alphabet; local policies regarding call signs allocated
- Uses of phonetic alphabet: enables quick identification of individuals; enables spelling of words during transmissions to avoid misunderstandings

7.3 Identify the benefits of teamwork in the private security industry
- Promotes safety
- Provides a professional and safe service and establishment
- Supports colleagues
- Promotes efficiency

7.4 State the principles of customer service
- Establishing rapport, acknowledging the customer, communicating information effectively, showing respect, listening to the customer and trying to meet their expectations
- Dealing with problems - acknowledge the customer, establish the customer's needs, put yourself in the customer's position, accept responsibility, involve the customer in the solution, see it through

7.5 Recognise diverse customer needs and expectations
- Types of customer - internal and external, direct and indirect
- Customer needs/expectations - e.g. information, assistance, directions
- Customers with particular needs - e.g. physical difficulties, learning difficulties, sensory impairment, English as second language, under influence of drugs and/or alcohol

LO8 Understand record-keeping relevant to the role of the security operative

8.1 State the importance of accurate record-keeping
- To comply with the law
- To provide a clear audit trail of the incident or accident
- To prevent you from having to rely on your memory

8.2 Identify the types of records that may need to be completed
- Incident records
- Accident records
- Searches and checks
- Logbooks

- Pocket notebooks
- Search/visitor/key registers
- Duty sheets
- Accident reports
- Lost/found property registers
- Message books
- Handover reports
- Other site-specific reports

8.3 Identify what information to include in records

- Who – the report is for/was written by
- What – happened/action was taken/was the result
- When – Day/date/time
- How – did it happen
- Where – place of incident
- Details of any other witnesses/people/injuries or property

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

Statement to be completed as part of the training and internally assessed with a sign off sheet submitted to Highfield to say this is completed.

- The implications of failing to complete the section 9 statement or using the required documents.
- The Police and Criminal Evidence (Northern Ireland) Order 1989
- Incidents requiring physical intervention/use of force, must be fully reported – including:
  - description of subject/s behaviour
  - other 'impact factors'
  - staff responses including description of physical interventions and level of force used
  - description of any injuries sustained
  - first aid and/or medical support provided
  - details of admission to hospital
  - support to those involved and follow up action required

8.5 State the process of attending court to give evidence

- Follow organisation's policies and procedures
- Follow any legal advice from representative
- Be punctual and prepared

LO9 Understand terror threats and the role of the security operative in the event of a threat

9.1 Identify the different threat levels

- The official source of UK Threat Level is (MI5) and their website is https://www.mi5.gov.uk/threat-levels. As well as knowing what each level means an operative would ideally need to know how it may impact the response level their location may have.
- LOW means an attack is highly unlikely
- MODERATE means an attack is possible, but not likely
- SUBSTANTIAL means an attack is likely
- SEVERE means an attack is highly likely
- CRITICAL means an attack is highly likely in the near future

- Have an understanding of how UK threat level may impact the response level for the location in which you are working.

9.2 Recognise the common terror attack methods

- Awareness of attack planning phases.
- Most current terrorist attack methodologies:
  - marauding terror attack (MTA), including firearms, knives, blunt objects, etc.
  - explosive device, including improvised explosive device (IED), person-borne improvised explosive device (PBIED). vehicle-borne improvised explosive device (VBIED), leave behind improvised explosive device (LBIED)
  - vehicle as a weapon (VAAW) also known as vehicle ramming
  - chemical, biological, radiological and nuclear (CBRN), including acid attacks.
  - cyber-attacks
  - insider threat

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

- Understand the role security operatives have to play during a terror attack.
- Understand what Run, Hide, Tell means for a security operative: keeping yourself safe and encouraging members of the public, who will look up to you, to follow you to a safe place
- Know and follow relevant procedure for your place of work, including the company's evacuation plan within the limits of your own authority.
- Use your knowledge of the location and making dynamic decisions based on available information to keep yourself and the public safe.
- Know the difference between evacuation and invacuation (lockdown), including the pros and cons of both options.
  - In both of these situations, the pros can very easily become cons. For example, evacuating a building due to fire tries to keep people safe but the con can be that people rush out and get injured or stand around outside which could result in accident. Conversely, taking people into a building for safety due to a terrorist act on the street can mean that they are all grouped together and could be seen as an easy target for other forms of terrorist activities.
- Report incidents requiring immediate response from the police on 999
- Know what information emergency response requires:
  - What you have seen and what has happened.
  - Who you saw, what they looked like, what they were wearing.
  - Where the situation happened and where you are.
  - When it happened.
- Awareness of emergency services response time
- Reporting suspicious activity that does not need immediate response to the Anti-Terrorist Hotline.
- Know who the public sector counter-terrorism experts are and how to access their information;
  - Centre for the protection of national infrastructure (CPNI)
  - National Counter Terrorism Security Office (NaCTSO)
- Awareness of current initiatives:
  - Run, hide, tell - keeping themselves safe and encouraging members of the public, who will look up to a person wearing a yellow vest, to follow them to a safe place.
  - ACT - Action Counter Terrorism
  - SCaN - See, Check and Notify

9.4 Identify the procedures for dealing with suspicious items

- HOT Principles:
  - hidden, obviously suspicious, typical
- 4 Cs:
  - confirm, clear, communicate and control
- Safety distance, including:
  - distance v suspicious item size (small items: 100m - large items or small vehicle: 200m - large vehicle: 400m)
  - how to visually represent safety distances (e.g. football field)
  - difficulty involved in setting up a safety distances and not use radio/mobile phone within 15 metres

9.5 Identify behaviours that could indicate suspicious activity

- Suspicious activity is any observed behaviour that could indicate terrorism or terrorism-related crime
- Hostile reconnaissance is the observing of people, places, vehicles and locations with the intention of gathering information to plan a hostile act
- Understand examples of what this might look like, including:
  - individuals taking particular interest in security measures, making unusual requests for information, testing security by breaching restricted areas, loitering, tampering with utilities
  - individuals avoiding security staff.
  - individuals carrying out activities inconsistent with the nature of the building or area.
  - individuals with forged, altered or stolen identity documents, documents in different names, with large amounts of cash, inappropriately dressed for season/location, taking photos or making drawings
  - parked vehicles with people inside, empty parked vehicles left unattended for long period
  - multiple sightings of same suspicious person, vehicle, or activity
- Understands actions that can deter or disrupt hostile reconnaissance, including:
  - ensuring a visible presence of vigilant security staff; frequent patrols but at irregular intervals
  - maintaining organised search procedures
  - ensuring emergency exits are secured when not in use to prevent unauthorised entry

9.6 Identify how to respond to suspicious behaviour

- Use your customer service skills to disrupt potential hostile reconnaissance
- Understand the importance of showing professional behaviour and visible security as a tool to deter hostile reconnaissance
- Know where to report suspicious behaviour including:
  - internal procedure for site
  - confidential (anti-terrorist) hotline: 0800 789 321
  - British Transport Police (BTP) 'See it, Say it, Sorted': text 61016 or call 0800 40 50 40
  - non-emergency: 101
  - ACT online reporting
  - Life-threatening emergency or requiring immediate response: 999

LO10 Understand how to keep vulnerable people safe

10.1 Recognise duty of care with regard to vulnerable people

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

10.2 Identify factors that could make someone vulnerable

- Vulnerable:
  - being under the influence of alcohol 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
  - mental ill-health
  - learning/physical disabilities
  - being elderly
  - being acutely ill
  - key behaviours associated with a range of invisible disabilities (physical, mental or neurological condition that limits a person's movements, senses or activities that is invisible to the onlooker)
- Indicators of child sexual exploitation: children and young people in the company of older people or antisocial groups, acting in an inappropriate and sexualised way; intoxicated; arriving and departing a location with different adults; getting into and out of several different cars

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

- Seeking help from other professionals, police, ambulance, street pastors, street marshals or representatives from any other scheme active in the area to help people
- Offer to call a relative or friend to give assistance
- Offer to call a licensed taxi to take the vulnerable person home
- Using 'safe havens' or other local initiatives run by organisations such as St John Ambulance
- Be aware of current safety initiatives e.g. 'Ask Angela' campaign
- Reporting indicators of child sexual exploitation:
  - Contact the police or call Crimestoppers
  - Report as soon as possible

10.4 Identify behaviours that may be exhibited by sexual predators

- Close monitoring of vulnerable people
- Buying drinks or gifts for vulnerable people
- Suspicious behaviour around certain times and venues
- Unusual use of technology, e.g. upskirting with phones

10.5 Identify indicators of abuse

- Restricting freedom of individuals
- Unexplained bruising
- Lack of confidence and insecurity
- Change in circumstances, e.g. cleanliness, appearance

10.6 State how to deal with allegations of sexual assault
- Follow organisation's policies and procedures
- Notify police
- Safeguard victim
- Separate victim from assailant
- Record and document all information

10.7 State 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 behaviour
- Explain the consequences if the anti-social behaviour continues
- Remain calm
- Ensure that your colleagues know about the situation and that you have back-up if needed
- Vigilance;
- High-profile patrols;
- Early intervention;
- Positive non-aggressive communication;
- Prompt reporting of incidents;
- Accurate recording of incidents;
- Liaison with police and other appropriate agencies.

LO11 Understand good practice for post-incident management

11.1 Identify sources of post-incident support available
- Sources of support through colleagues, management and counsellors
- Publications, internet
- Help-lines (eg Samaritans)
- Other support eg citizen's advice/trade unions

11.2 State why accessing support following an incident is important
- Reducing the chances of long-term problems such as depression, anxiety, fear, post-traumatic stress
- Helps you to reflect on the incident and evaluate your actions

11.3 State the benefits of reflecting on incident
- Areas for improvement can be identified
- Preventing reoccurrence of the same problem
- Organisations can use data for licensing hearings
- Recognising trends
- Recognising poor and/or good practice
- Sharing good practice
- Making improvements
- Improving procedures for incident management
- Identifying common response to situations

11.4 Identify why it is important for security operatives to contribute to improving practice

- Promotes professional service
- Increases safety for staff
- Promotes teamwork
- Increases safety for customers
- Identifies procedures or methods to deal with situations effectively

Unit 2: **Principles and Practices of working as a CCTV operator in the private security industry**

Unit number: K/617/9261
Credit: 1
Min. contact time: **13**
GLH: 13
Level: 2

Learning Outcomes	Assessment Criteria
The learner will	***The learner can***
1. Understand the purpose of surveillance (CCTV) systems and the roles and responsibilities of the control room team and other stakeholders	1.1 Identify the different uses of public space surveillance (CCTV) systems 1.2 State the roles and responsibilities of each member of the control room team 1.3 Identify the roles of other stakeholders in public space surveillance (CCTV) systems 1.4 State how to work effectively with a range of stakeholders and other agencies
2. Understand the different types of legislation and how they impact on Public Space Surveillance (CCTV) operations	2.1 Identify how the Data Protection Act impacts on the role of a CCTV Operator 2.2 Identify how the Freedom of Information Act impacts on public space surveillance (CCTV) operations 2.3 Identify how the Protection of Freedoms Act impacts on public space surveillance (CCTV) operations 2.4 Identify how human rights impact on public space surveillance (CCTV) operations 2.5 Identify how the principles of covert surveillance impact on public space surveillance (CCTV) operations 2.6 Identify how the offence of voyeurism impacts on public space surveillance (CCTV) operations 2.7 Recognise the impact of Codes of Practice on public space surveillance (CCTV) 2.8 Identify how the use of unmanned aerial vehicles (UAV) is controlled
3. Understand the importance of operational procedures in public space surveillance (CCTV) operations	3.1 State why operational procedures are necessary to public space surveillance (CCTV) operations 3.2 Identify the key elements of an operational procedures' manual 3.3 State how the operational procedures manual impacts on public space surveillance (CCTV). 3.4 State the procedure for creating an evidential audit trail

Learning Outcomes	Assessment Criteria
The learner will	*The learner can*
4. Understand how public space surveillance (CCTV) systems equipment operates	4.1 Identify how the different components of a surveillance system operate 4.2 Identify the purpose of functional checks on control room equipment
5. Understand surveillance techniques	5.1 Explain a range of surveillance techniques 5.2 State the standards for capturing evidential images 5.3 State actions to take when dealing with multiple incidents
6. Understand different types of incidents and how to respond to them	6.1 Recognise the difference between a crime and non-crime incident 6.2 Identify the CCTV Operator's response to a crime and non-crime incident
7. Understand health and safety in the CCTV environment	7.1 State the guidelines for CCTV operators under the display screen equipment regulations 7.2 Identify the factors in CCTV operations which may create stress for operators and how to deal with them 7.3 Identify specific risks and controls when working in CCTV operations
8. Demonstrate operational use of CCTV equipment	8.1 Demonstrate functional checks on control room equipment 8.2 Demonstrate how to use surveillance equipment 8.3 Demonstrate surveillance techniques 8.4 Demonstrate effective use of communication devices 8.5 Obtain an evidential image
9. Produce evidential documentation	9.1 Produce documents required for the audit trail

Assessment Guidance

Please find guidance below regarding the practical assessments associated with this unit. All practical assessment templates are available from the Download Area of the Highfield Qualifications website.

- **AC 2.6: Identify how the offence of voyeurism impacts on public space surveillance (CCTV) operation**
- **AC 5.1: Explain a range of surveillance techniques**
- **AC 5.2: State the standards for capturing evidential images**

- **AC 5.3: State actions to take when dealing with multiple incidents**
- **AC 7.3: Identify specific risks and controls when working in CCTV operations**
- **AC 8.1: Demonstrate functional checks on control room equipment**
- **AC 8.2: Demonstrate how to use surveillance equipment**
- **AC 8.3: Demonstrate surveillance techniques**
- **AC 8.4: Demonstrate effective use of communication devices**
- **AC 8.5: Obtain an evidential image**
- **AC 9.1: Produce documents required for the audit trail**

This unit is assessed by the completion of a workbook. This workbook is designed to enable the learner to show understanding and knowledge within their role and demonstrate their skills through practical application.

Section 1 of this workbook contains six knowledge questions in relation CCTV operations and **MUST** be completed by the learner only and internally marked by the assessor. To pass this section learners will need to achieve 12/15 (80%).

Learners are expected to complete this section before participating in their practical operation of CCTV equipment assessment.

Section 2 focuses on observation of the learner demonstrating practical use of a CCTV system. The assessor should indicate on the documentation what the learner has completed and provide comments. It is the judgement of the assessor as to whether the learner has achieved this section to a satisfactory standard.

Centres must make a record of the time each learner spends on the practical observation aspect in order to confirm that the mandatory hours are complied with.

The practical observation assessment is conducted on a 1-1 basis, which covers LO8 (approximately 25 mins), the candidate must be video recorded, when completing their final practical assessment.

The collation of evidence and completion of documentation (to cover AC 9.1) can be conducted as a group.

Learners are required to produce evidence to support the assessment, as detailed within the tutor, assessor and IQA (TAI) support pack.

Indicative Content

LO1 Understand the purpose of a surveillance (CCTV) systems and the roles and responsibilities of control room team and other stakeholders

1.1 Identify the different uses of public space surveillance (CCTV) systems

- Assisting in the prevention, detection and reduction of crime, disorder and anti-social behaviour
- Assisting in promotion of community/public safety
- Monitoring traffic flow and assisting in traffic management issues
- Assisting in civil emergencies and counterterrorism

- Assisting in the prosecution of offenders

1.2 State the roles and responsibilities of each member of the control room team

- Roles include:
  - Team worker: operator, supervisor, manager, systems manager, technical support staff
- Responsibilities of each include:
  - Observing, recording, reporting
- Other responsibilities include:
  - Following Home Office guidance
  - Knowing the difference between private and public areas
  - Privacy blanking
  - Knowing what can/cannot be recorded

1.3 Identify the roles of other stakeholders in public space surveillance (CCTV) systems

- Other stakeholders:
  - Police, customs, health and safety, ambulance, fire and other members of the team during CCTV operations
- Communication in response to CCTV operations

1.4 State how to work effectively with a range of stakeholders and other agencies

- Working effectively can include:
  - Pass and receive information from other stakeholders: Police, other members of the CCTV team and other emergency services during CCTV operations
  - Dealing with a multi-incident and multi-agency operation.
- Third parties to include:
  - Emergency services
  - Statutory agencies
  - Media
- Types of assistance:
  - Providing intelligence and information
  - Tracking, searching and securing areas
  - Crowd control/evacuation
  - Recording evidence
- Utilising:
  - Radio, phone, personnel
  - Dedicated person in room/dedicated telephone line

LO2 Understand the different types of legislation and how they impact on Public Space Surveillance (CCTV) operations

2.1 Identify how the Data Protection Act impacts on the role of a CCTV Operator

- The meaning of "confidentiality" as it applies to the role of a CCTV operator:
  - Compliance with 6 principles of the Data Protection Act
  - Not disclosing information to any unauthorised persons relating to all operational aspects of the system and data security
  - No unauthorised recording e.g. using mobile phones or similar devices
  - No unauthorised copying of footage
  - Body-worn cameras
  - UAVs - Drones

- Repercussions of breaches e.g.:
  - Dismissed, fines and potential prosecution

2.2 Identify how the Freedom of Information Act impacts on public space surveillance (CCTV) operations

- Who it applies to:
  - Local councils and other public bodies only
  - Who can request information under the Act
  - Who and what type of information, only data held on individuals (subject access)
  - Exemptions national security

2.3 Identify how the Protection of Freedoms Act impacts on public space surveillance (CCTV) operations

- The role of Surveillance Camera Commissioner:
  - To promote the Surveillance Camera Code of Practice and review its operation and impact

2.4 Identify how human rights impact on public space surveillance (CCTV) operations

- The articles of the Human Rights Act, that impact on the role
- Main articles:
  - Article 6: right to a fair trial
  - Article 8: right to privacy and family life
  - Article 14: prohibition of discrimination
- Articles are:
  - Absolute, limited and qualified
- Impact on CCTV operations such as necessity, proportionate, legal and non-discriminatory

2.5 Identify how the principles of covert surveillance impact on public space surveillance (CCTV) operations

- Purpose of Regulation of Investigatory Powers Act (RIPA):
  - Authorisation of covert/ directed surveillance
- Circumstance for authorisation:
  - Who can authorise e.g., police
- Definition of surveillance (difference between Directed and Intrusive Surveillance)
  - Directed:
    Directed surveillance is covert surveillance that is not intrusive and is carried out in relation to a specific investigation or operation
  - Intrusive:
    Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle (and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device)

2.6 Identify how the offence of voyeurism impacts on public space surveillance (CCTV) operations

- Safeguarding requirements:
  - Safeguarding children and young people, and others including voyeurism, limits what can view and record

- What considerations to take before viewing CCTV material
- Voyeurism falls under the Sexual Offences Act 2003

2.7 Recognise the impact of Codes of Practice on public space surveillance (CCTV)

- Information contained in the Information Commissioner's CCTV Code of Practice:
  - Is a public document that governs how processes and procedures for CCTV operators are developed
  - Ensures evidence admissible in court
  - Increases protection and confidence of the public
  - Ensures compliance with legislation
  - Raise standards
  - Improve efficiency
- Surveillance camera code of practice:
  - The 12 guidance principles and how each principle affects the operator's actions and the procedures they must follow
  - SIA Standards of Behaviour
  - Company procedures, manuals and assignment instructions; industry standards

2.8 Identify how the use of unmanned aerial vehicles (UAV) is controlled

- Safeguarding Role of the Civil Aviation Authority (CAA) and the Air Navigation Order is to:
  - Monitor the use of UAV within restricted airspace (Airports)
- The CCTV operative needs to be:
  - Aware of the reporting process and;
  - Communicate sightings to the appropriate services

LO3 Understand the importance of operational procedures in public space surveillance (CCTV) operations

3.1 State why operational procedures are necessary to public space surveillance (CCTV) operations

- Value of codes, procedures and guidelines:
  - Public: reassurance, protects; partners: improving efficiency, clear working relationships.
  - Ensuring integrity of system and personnel that run the system
  - Reassuring the public
- Definition of operational procedures:
  - Establishes best practice
  - Compliance with legislation
  - Protection of public
  - Protect the CCTV system and staff from complaints and allegations of malpractice and expectations under the Data Protection Act

3.2 Identify the key elements of an operational procedures' manual

- Information found in CCTV Operations manual can include the following:
  - Access control to control room
  - Emergency Procedures
  - Health and Safety
  - Proactive use of CCTV

- Duties and Shift Patterns
- Image management
- Communications and Radios
- Legal guidance
- Key Handling
- Fault reporting methods
- System failure and actions
- System Maintenance
- Essential/useful contact numbers
- Releasing Recorded Information

3.3 State how the operational procedures manual impacts on public space surveillance (CCTV)

- System must be:
  - Operated, controlled, maintained within a control room to a set procedure
  - Enables standardisation and consistency for all operatives to work in the same manner
  - Establishes the boundaries of the procedures

3.4 State the procedure for creating an evidential audit trail

- Importance of accurate and detailed note taking and record keeping:
  - Admissible in court, audit trail
  - Guidelines for writing notes and records
  - Consequences of incorrect record keeping
- Ensure rough notes also kept as can be used as evidence:
  - Master, copy, bag and tag

LO4 Understand how public space surveillance (CCTV) systems equipment operates

4.1 Identify how the different components of a surveillance system operate

- Main components of a surveillance system are:
  - Cameras, lenses, operator control
  - Keyboard/touch screen
  - Display screens
  - Transmission system
  - Video management system (VMS) recording systems
- Emerging technologies are:
  - Artificial Intelligence (AI)
  - Automatic Facial Recognition (AFR)
  - Automatic Number Plate Recognition (ANPR)
  - Biometrics, Body Worn Cameras (BWC)
  - UAV (Drone)

4.2 Identify the purpose of functional checks on control room equipment

- Ensure all equipment is operational and in full working order:
  - Minimises system failures
- Equipment to be checked:
  - Cameras
  - Control equipment (keyboards/joystick)
  - Monitors
  - Recording equipment and computers

- Log faulty equipment in accordance with operational procedures

LO5 Understand surveillance techniques

5.1 Explain a range of surveillance techniques

- Surveillance techniques include:
  - Pattern recognition
  - Activity profiling
  - Pro-active and reactive surveillance techniques
  - Planning surveillance
  - Hotspots (high-risk areas)
  - Human behaviours:
    - suspicious activity
    - body language
  - Situational awareness
  - Incidents and occurrence
  - Lost contact drills

5.2 State the standards for capturing evidential images

- Images dimensions for evidential purposes
- Quality/size that could be used:
  - Identification 100%
  - Recognition 50%
  - Observation 25%
  - Detection 10%
  - Vehicles 50%
- Quality and frame rate can affect evidential image through high compression levels, low quality and frame rate
- System performance in adverse conditions:
  - Fog/mist
  - Snow
  - Obstructions (foliage, signs)
  - Low light

5.3 State actions to take when dealing with multiple incidents

- Work as a team
- Prioritising of incidents
- Maximise use of available equipment
- Communication with team and statutory enforcement agencies (includes notifying if applicable)
- Completing relevant documentation
- Post-incident actions

LO6 Understand different types of incidents and how to respond to them

6.1 Recognise the difference between a crime and non-crime incident

- Non-criminal:
  - Crowd control

- Evacuation
- Missing person
- Accident
- Fire
- Traffic
- Flood
- Safety issues

- Criminal:
  - Theft
  - Robbery
  - Burglary
  - Assault
  - Criminal damage
  - Drug related

6.2 Identify the CCTV Operators response to a crime and non-crime incident

- Actions to be taken when dealing with multiple incidents to a crime and non-crime incident:
  - Communication with police, emergency services, supervisors, health and safety executive and local authority
- Graded Response:
  - Immediate – Risk to life
  - Routine – May need action
  - Deferred – No immediate action required
- Maintain a record of all incidents in the appropriate incident log

LO7 Understand health and safety in the CCTV environment

7.1 State the guidelines for CCTV operators under the display screen equipment regulations

- Health and Safety (Display Screen Equipment) Regulation 1992
  - Carry out risk assessment of work station
  - Regular breaks
  - Eyesight test

7.2 Identify the factors in CCTV operations which may create stress for operators and how to deal with them

- Different causes:
  - Work-related
  - Non-work related
- Key indicators:
  - Physical – aches and pains, etc.
  - Behavioural – mood swings, etc.
  - Emotional – worrying, anxiety, etc.
  - Alleviating stress
  - Stress management

7.3 Identify specific risks and controls when working in CCTV operations

- Specific risks inside and outside the control room can include:
  - Fire
  - Bomb Threats/ Improvised Explosive Device (IED)

- Trip/slip hazards
- Electrical hazards

- Purpose of risk assessments to include:
  - Identifying and determining risk
  - Minimising risk to reduce and prevent accident
  - Responsibility for complying with health and safety regulations

LO8 Demonstrate operational use of CCTV equipment

8.1 Demonstrate functional checks on control room equipment he importance of accurate record-keeping

- Functional checks on CCTV control room equipment:
  - Cameras
  - Control equipment (keyboard/joystick)
  - Monitors
  - Recording equipment
  - Computer
  - Workstation
- Produce a completed fault log, (include in folder)
- Communicate using a range of devices

8.2 Demonstrate how to use surveillance equipment

- Use CCTV control room equipment including the use of:
  - Controllers
  - Recording devices
  - Monitors
  - Video Management Systems (VMS)
  - Use of Pan, Tilt, Zoom (PTZ)
  - Body-worn camera (BWC) - as applicable
  - UAV (Drone) as applicable
- Overcome problems caused by weather

8.3 Demonstrate surveillance techniques

- Prioritise during multiple incidents
- Detect and track/follow suspect on foot or in a vehicle:
  - Locate, track
  - Secure evidence and images
  - Use of Pan, Tilt, Zoom (PTZ)
- Lost contact drill and searching:
  - Last location check
  - Use of multiple cameras
  - Methodical and systematic searching
  - Use of Pan, Tilt, Zoom (PTZ) to conduct zoom in/out 360-degree checks

8.4 Demonstrate effective use of communication devices

- Use different communication methods to pass and receive information
- Give clear and accurate descriptions of people, vehicles and events:
  - Suspicious activity
  - Description of individual persons
  - A group

- A vehicle
- An incident
- Provide location and directions

- Individual:
  - Gender
  - Age
  - Build/weight
  - Height
  - Clothing
  - Distinguishing features
  - Ethnicity, hair, etc.
- Vehicle:
  - Car colour
  - Registration
  - Make/type (as a minimum)
- Type of incident:
  - Location
  - Who/what is involved
  - Describe event as it unfolds
  - Complete relevant documentation

8.5 Obtain an evidential image

- Produce images of quality/size that could be used as evidence:
  - Identification 100%
  - Recognition 50%
  - Observation 25%
  - Detection 10%
  - Vehicles 50%

LO9 Produce evidential documentation

9.1 Produce documents required for the audit trail

- Copy of rough notes taken during the incident
- Incident report
- Copy of recorded images (practical assessment)
- Print log
- Evidence labels
- Evidence review log
- Evidence handover document
- Fault log (as 8.1)
- Statement detailing actions

Appendix 3: Sample assessment material

Working in the Private Security Industry Witness Statement

Learner name:		Centre no:	

AC 8.4: Demonstrate the accurate completion of an evidential statement (Section 9 Statement)
Witness Statement (CJ Act 1967, s.9 MC Act 1980, ss. 5B (3a) & MC Rules 1981
Statement of: **Age if under 18:..... (if over 18 insert 'Over 18')** **Occupation:** .....
This statement (consisting of (...) pages each signed by me) is true to the best of my knowledge and belief and I make it knowing that, if it tendered in evidence, I shall be liable to prosecution if I wilfully stated anything in it which I know to be false or do not believe to be true. **Dated the:** ..... **Signature:** .....
Signature: ..... **Signature witnessed by:** .....

Working as a CCTV Operator Section 2 – Practical Operation of CCTV Equipment Assessment Record

Learner name:		Centre no:	

Did the learner meet the following criteria:	Yes	No	AC Ref.	Supporting Evidence
Carry out functional checks of the CCTV System			8.1	
Carry out equipment fault procedures				
Use keypads and joysticks to operate cameras, monitors and associated equipment			8.2	
Whilst operating a CCTV system be able to liaise with other agencies and take notes as appropriate			8.4 9.1	
Identify body language and behaviours that could indicate unusual or suspicious activity			8.4	
Whilst operating the CCTV System able to give clear and accurate descriptions of people, vehicles and events				
Use of cameras to search the outside of buildings, streets and open spaces for suspicious items			8.3	
Using a CCTV system detect and track/follow a suspect on foot or in a vehicle				
Whilst operating the CCTV system, carry out a lost contact drill				
Record images onto storage media in an evidentially sound manner			8.5 9.1	
Produce images for evidential purposes			8.5	
Complete documentation ensuring audit trail is sound This should include: • Copy of rough notes made during incident • Incident report • Copy of video recording (assessment) • Print Log • Evidence labels • Evidence Review Log • Evidence handover document • Fault Log • Statement detailing actions			9.1	

Appendix 4: Standards of behaviour for security operatives

https://www.sia.homeoffice.gov.uk/Documents/sia-standards-of-behaviour.pdf

Personal appearance

A security operative should at all times:

- wear clothing which is smart, presentable, easily identifies the individual as a security operative, and is in accordance with the employer's guidelines

Professional Attitude and Skills

A security operative should:

- greet visitors to the premises in a friendly and courteous manner
- act fairly and not discriminate on the grounds of gender, sexual orientation, marital status, race, nationality, ethnicity, religion or beliefs, disability, or any other difference in individuals which is not relevant to the security operatives' responsibility.
- carry out his/her duties in a professional and courteous manner with due regard and consideration to others.
- behave with personal integrity and understanding
- use moderate language, which is not defamatory or abusive, when dealing with members of the public and colleagues
- be fit for work and remain alert at all times
- develop knowledge of local services and amenities appropriately

General Conduct

In carrying out his/her duty, a security operative should:

- never solicit or accept any bribe or other consideration from any person.
- not drink alcohol or be under the influence of alcohol or drugs
- not display preferential treatment towards individuals
- never abuse his/her position of authority
- never carry any item which is or could be considered to be threatening
- report all incidents to the management
- co-operate fully with members of the police and partners, local authority, Security Industry authority, and other statutory agencies with an interest in the premises or the way they are run.

Organisation/Company Values and Standards

A security operative should:

- adhere to the employing organisation/company standards
- be perceptive of the employing organisation/company culture and values
- contribute to the goals and objectives of the employing organisation/company.