Appeals Policy

Defence Security is a progressive training organisation providing mandatory training to a range of organisations. We provide education and training and assessing qualifications through BIIAB.

At Defence Security we are committed to providing high quality training and qualifications, and to ensuring that equality of opportunity underpins all aspects of our work.

This policy relates to complaints that our customers, students and suppliers may have about our organisation and sets out our formal procedure for dealing with such complaints.

It is important that all appeals are raised directly with Defence Security.

Our appeals policy is a four stage process, each process is detailed below, most complaints will be resolved to a satisfactory standard at stage one.

If the complaint is not resolved at stage one then it should be escalated to stage two and if not resolved again it should be escalated to stage three, finally if not resolved at the third stage the final stage should be used.

Stage one:

- Complaint is raised directly with the assessor conducting the assessment, who will deal with the concern/complaint at the time that it is raised.
- The usual course of action would be for the candidate to repeat the assessment.

Stage two:

- If the candidate is still not happy with the outcome of the second assessment they should raise this as soon as possible with the course tutor or centre manger, details of the centre manager are provided here:
- Abdul Basit, Defence Security, St Georges Community Hub, Great Hampton Row, Birmingham, B19 3JG, 07859458057, basit@defence-security.co.uk, www.defence-security.co.uk.
- We will aim to resolve all complaints within 10 working days in writing.

Stage three:

- Only if the candidate is still not happy with the outcome from the training centre can they refer their appeal to BIIAB, who will carry out an investigation into the complaint and will contact the complainant with the results of their investigation.
- BIIAB can be contacted by phoning 0115 854 1620.

Stage four:

- Stage four is the final stage of the appeal, if your appeal has not been resolved, you can take your appeal to Ofqual, CCEA regulation or QiW using their appeals procedure, however, you must have exhausted all options above.

You can make us aware of your complaint by letter, phone or email.

Office of Qualifications and Examinations Regulation
Earlsdon Park,
53-55 Butts Road,
Coventry
CV1 3BH

Telephone: 0300 303 3346
(Lines are open Monday to Friday, 9.00am to 5.00pm)

Textphone: 0300 303 3345

Fax: 0300 303 3348

Email: info@ofqual.gov.uk

Qualifications Wales
Q2 Building
Pencarn Lane
Imperial Park
Coedkernew
Newport
NP10 8AR

Email: contact@qualificationswales.org

Policy: http://qualificationswales.org/media/1444/281015-reg-complaints-awarding-bodies.pdf

CCEA Regulation
Marisa Getgood *(Complaints Co-ordinator)*
CCEA
29 Clarendon Road
Clarendon Dock
Belfast BT1 3BG
Email: mgetgood@ccea.org.uk
Telephone: +44 (0)2890 261407
Fax: +44 (0)2890 261234
Text Phone: (0)2890 242063

You need to provide regulators with the following information:

- What the complaint is about

- Your full name and candidate number (if you have one)
- The training provider's name and number
- The name of the awarding organisation or exam board
- The qualification or unit title and code number
- Copies of any relevant supporting documents.

Ofqual promise to:

- acknowledge receipt of your complaint within two working days of receiving it
- give you a full response within 30 working days.

Defence Security will keep a written record of all appeals made and the outcomes, this will be made available to any inspectors or other organisations that conduct Quality Assurance based audits.

Our primary goal is to provide high quality customer focused training and qualifications; therefore we aim to have very few appeals to our decisions and certainly aim to resolve any appeals within our company.

This policy was approved by: Abdul Basit, April 2022

Review Due: April 2024

Assessment And Internal Verification Policy

Policy

Senior management supports the quality assurance process and will ensure that the requirements of the Awarding Body are followed.

The roles and responsibilities of assessors and internal verifier are recognised as being essential to the delivery and quality assurance of Defence Security. Sufficient time will be allocated so that the assessment and internal verification team can carry out their duties effectively.

Competent and qualified assessors and internal verifiers will be responsible for the delivery of qualifications. A training programme to train new assessors will be put in place in line with the codes of practice.

Satellite systems and procedures will follow those of Defence Security and regular checks will be made to ensure this.

Rationale

The quality assurance of qualifications can only be maintained by competent and qualified assessors and internal verifiers, working to the national codes of practice and BIIAB requirements.

Context in which this policy operates

Awarding body approval depends on all the quality assurance criteria being in place and procedures designed to ensure assessors and internal verifiers receive information from the awarding body on a regular basis.

Assessment and internal verification strategies must be in line with the codes of practice and awarding body recommendations.

Awarding body approval depends on Defence Security having robust administrative systems to ensure efficient record keeping and retention of identified records, relevant policies in place and evaluation procedures, to support the assessment and internal verification process in sustaining continuing good practice.

Clear indication of roles and responsibilities allocated to named individuals for all processes involving candidates` assessment and internal verification must be available as reference for all staff and auditors.

Sampling

The internal Verifier must:

Ensure that monitoring of the qualification is carried out on an ongoing basis, appropriate to the candidate and assessment activities taking place within the IV's area of responsibility.

Consider the sample size so that it ensures reliability and develop a sampling plan to support the procedure.

Ensure that the sampling process covers each assessor in the team, each unit in the qualification, the full range of assessment methods, and across as wide a range of candidates as possible.

Ensure that the sampling process takes account of:

- Workload and experience of the assessor
- Range of assessment methods
- Candidate cohorts
- Old and new standards (if appropriate)

When sampling, check assessment records, assessment methods used by the assessor and verify that the evidence produced by the candidate supports the assessment decisions.

Witness Testimony should be checked for authenticity by the assessor.

Sample assessment methods used and ensured that direct assessment of natural performance is used wherever possible.

Where action is identified, ensure that target dates are agreed, and feedback is received from the assessor.

Ensure unqualified assessors are countersigned by qualified assessors.

Indicate on the portfolio sampling if internal verification is formative and summative internal verification.

Standardisation of Assessment

The internal verifier should:

Plan and record dates of standardisation and other relevant meetings/activities to cover at least the next six months of the assessment and internal verification cycle.

Hold regular standardisation meetings with all assessors.

Select a range of activities to take place during such meetings including:

- Selecting a unit where assessors have the opportunity to discuss different approaches and give views on how the problems can be overcome.
- Concentrate on one particular type or source of evidence
- Look at the implications of new standards
- Look at alternative assessment strategies

Ensure that any assessor training or development needs identified during these meetings is actioned.

Discuss any changes/updates to the Awarding Body procedures or qualifications and ensure that all assessors understand the implications of these and take any necessary action.

Maintain minutes of standardisation meetings. Where any action is required by an assessor, ensure that this action is taken by the time allocated and is reviewed at the next meeting. Make copies of the minutes available to the external verifier highlighting any sections of the minutes which are particularly relevant.

INTERNAL VERIFICATION PROCEDURE

1) Managing the quality assurance of the assessment and internal verification of qualifications

Senior management should recognise the role and responsibilities of the internal verifier and allocate sufficient time for all duties to be completed effectively.

A nominated person must be allocated by senior management to be responsible for operating and reviewing Defence Security's systems and internal verification. This person must hold a nationally accredited internal verifier award, continue to work consistently to the standards at all times and ensure new internal verifiers operate similarly.

Defence Security must maintain copies of certificates for assessors who have achieved a nationally accredited assessor award for assessors and internal verifiers. Regular updates/information should be supplied to internal verifiers as necessary.

2) Allocation of assessors

The internal verifier must:

Ensure that all assessors have sufficient relevant and current occupational competence, understand the relevant national standards, hold or are working towards relevant nationally accredited assessor awards. Where assessors are 'working towards' ensure that target dates for achievement are specified and are within required timescales.

Ensure that only qualified assessors sign off assessment decisions by allocating a named counter signatory/mentor, who is a qualified, experienced assessor to all unqualified assessors joining the team.

Ensure that any assessor training and development need, identified as a result of the counter signatory is recorded, and passed on to the staff development officer in writing.

Maintain relevant details including copies of qualifications, occupational competence records and CVs for all assessors and internal verifiers on the team. Regular updates should be made as necessary.

Provide guidance and support for new or inexperienced assessors and ensure that any training needs are met to achieve the nationally accredited assessor award.

Ensure that information for the monitoring of equal opportunities and special needs is gathered at the point of candidate registration and is entered onto Defence Security's management information system (MIS). Such information should be analysed regularly against candidate achievement.

Where assessment has been carried out by the internal verifier, the allocation of another qualified internal verifier to internally verify these assessments should be arranged. It is recommended that internal verifiers do not internally verify each other's assessments.

Ensure that the Awarding Body criteria for certification claims, including direct claims are met in full.

3) Sampling

The internal verification must:

Ensure that the sampling process covers each assessor in the team, each unit in the qualification, the full range of assessment methods, and across as wide a range of candidates as possible.

Ensure that the sampling process takes account of:

- Each assessor's experience, workload, and location
- Problem or key units, possibly identified in the standardisation meetings
- The full range of assessment methods relevant to the qualification
- Candidate cohorts, e.g., full/part time, different employers, different programme start dates
- Old and new standards (if appropriate), looking out for any confusion in assessments ensuring candidates are being assessed to the correct set of standards

Finalise arrangements before each sampling session as follows:

- Date, time, and venue
- Personnel involved (i.e., assessors, candidates (internal verifier/candidate interview form) and workplace personnel, if appropriate)
- Portfolios to be made available, including assessment documentation and relevant specimen signature lists
- Other alterative assessment methods, if used
- Location of evidence if not contained in paper-based portfolio.

When sampling, check assessment records, assessment methods used by the assessor and verify that the evidence produced by the candidate supports the assessment decisions. Check:

- Assessment records are completed accurately, signed, dated, and maintained for each candidate sampled
- Signatures are authentic and that those on assessment records and portfolio. Evidence is held on the witness status list
- Initially with new assessors, 100 % sampling will be done until satisfied that all evidence is current, sufficient, authentic, valid, and consistent and that the judgement of the assessor is fair and reliable
- Assessment decisions taken by arranging checking and countersigning process for trainee assessors
- Assessment decisions meet the national standards and are in line with Awarding Body and the organisation's policies.

Carry out observation of direct assessment (observation) and indirect assessment (examination of evidence) for a minimum of one observation per assessor, ensuring that all assessors are covered over an annual cycle. Ensure trainee assessors are observed a sufficient number of times, until satisfied that the decisions and requirements of the assessor are fair and reliable.

Record the results of the observation – Evidence Report Form

Discuss results of observation with the assessor, agree actions and obtain signature of assessor.

Record that the observation of assessment has taken place - internal verification planning schedule.

Interview a sample of candidates to ensure they are aware of and satisfied with, the assessment process.

Evaluate feedback from candidates and discuss with assessors and feed into Defence Security's evaluation process.

Ensure that any assessor training or development need identified during this process is passed on promptly to the staff development officer, in writing.

4) Interim Sampling (Formative IV)

Sample portfolios as part of an evaluation process to ensure the quality of formative assessment practice. This should be carried out at various stages of assessment e.g.:

- Before assessment decisions have been made on a unit
- looking at portfolios with one or two units
- looking at assessments of new assessors
- checking the countersigning process.

Ensure that any assessor training or development needs identified during this process is passed on to the staff development officer, in writing.

Complaints Policy

Defence Security is a progressive training organisation providing mandatory training to a range of organisations. We provide education and training and assessing qualifications through BIIAB.

At Defence Security we are committed to providing high quality training and qualifications, and to ensuring that equality of opportunity underpins all aspects of our work.

This policy relates to complaints that our customers, students and suppliers may have about our organisation and sets out our formal procedure for dealing with such complaints.

It is important that all complaints are raised directly with Defence Security.

Our complaints policy is a four stage process, each process is detailed below, most complaints will be resolved to a satisfactory standard at stage one.

If the complaint is not resolved at stage one then it should be escalated to stage two and if not resolved again it should be escalated to stage three, finally if not resolved at the third stage the final stage should be used.

Stage one:

- Complaint is raised directly with the trainer/assessor conducting the course, who will deal with the complaint at the time that it is raised.
- If the complaint is not about a course but about another aspect of our business, then the complaint should be raised with the staff member the customer is in communication with.

Stage two:

- Complaint should be referred to Defence Security head office where there is a named contact who deal with complaints, they can be contacted, in writing by using the following details:
- Abdul Basit, Defence Security, St Georges Community Hub, Great Hampton Row, Birmingham, B19 3JG,07865361038, basit@defence-security.co.uk, www.defence-security.co.uk.
- We will aim to resolve all complaints within 10 working days in writing.

Stage three:

- Complaints should be referred to BIIAB, who will carry out an investigation into the complaint and will contact the complainant with the results of their investigation.
- Qualifications Network can be contacted by phoning 0115 854 1620.

Stage four:

- Stage four is the final stage of the complaint, if your complaint has not been resolved, you can take your complaint to Ofqual.
- You can make us aware of your complaint by letter, phone or email.

Office of Qualifications and Examinations Regulation

Earlsdon Park,
53-55 Butts Road,
Coventry
CV1 3BH

Telephone: 0300 303 3346
(Lines are open Monday to Friday, 9.00am to 5.00pm)

Textphone: 0300 303 3345

Fax: 0300 303 3348

Email: info@ofqual.gov.uk

Qualifications Wales

Q2 Building
Pencarn Lane
Imperial Park
Coedkernew
Newport
NP10 8AR

Email: contact@qualificationswales.org

Policy: http://qualificationswales.org/media/1444/281015-reg-complaints-awarding-bodies.pdf

CCEA Regulation

Marisa Getgood *(Complaints Co-ordinator)*
CCEA
29 Clarendon Road
Clarendon Dock
Belfast BT1 3BG

Email: mgetgood@ccea.org.uk

Telephone: +44 (0)2890 261407

Fax: +44 (0)2890 261234

Text Phone: (0)2890 242063

You need to provide regulators with the following information:

- What the complaint is about
- Your full name and candidate number (if you have one)
- The training provider's name and number
- The name of the awarding organisation or exam board
- The qualification or unit title and code number
- Copies of any relevant supporting documents.

Regulators promise to:

- acknowledge receipt of your complaint within two working days of receiving it
- give you a full response within 30 working days.

Defence Security will keep a written record of all complaints and compliments made about our business, this will be made available to any inspectors or other organisations that conduct Quality Assurance based audits.

Our primary is to provide high quality customer focused training and qualifications; therefore we aim to have very few complaints and certainly aim to resolve any complaints within our company.

This policy was approved by: Abdul Basit, April 2022

Review Due: April 2024

Conflict Of Interest Policy

Purpose
The purpose of this policy is to provide guidance to relevant individuals and organisations on handling possible conflicts of interest that may arise at Defence Security.

This policy applies to all staff and other individuals whenever they interact or potentially interact with any of Defence Security's operations.

This Policy:

- Defines what is meant by conflict of interest sets out the roles and responsibilities for managing conflict of interest

- Illustrations of potential conflict of interest situations.

Scope:
It is the policy of Defence Security that each individual working within or acting on behalf of the company must be free from conflicts of interest that could adversely affect their judgement or objectivity to the organisation in conducting business activities and assignments.

Defence Security recognises that each individual working within or acting on behalf of the organization may take part in legitimate financial, business, charitable and other activities outside of their recognised roles at Defence Security, but any potential conflict of interest raised by those activities must be acknowledged, disclosed, and in relevant cases properly managed.

It is the responsibility of each individual or organisation working within or acting on behalf of Defence Security to recognise situations in which they have a conflict of interest, or might reasonably be seen by others to have a conflict; to disclose this conflict and to take such further steps as may be appropriate and set out in more detail under the procedure below.

Definition of Conflict of Interest
A conflict of interest is a situation in which an individual, or organisation, has competing interests or loyalties. Conflicts of interest can arise in a variety of circumstances, and it is possible that people working alongside and/or for Defence Security may encounter potential conflicts of interest from time to time.

It is not possible to provide a definitive list of examples of conflicts of interest that could compromise the integrity of Defence Security.

However, the following situations could lead to perceived or actual conflicts of interest;

- When an individual has a position of authority in one organisation which conflicts with his or her interests in another organisation.

- When an individual has personal interests that conflict with his/her professional position at Defence Security.

- A conflict of interest may generally be defined as a conflict between the official responsibilities of a tutor, assessor, and internal verifier and any other interests the particular individual may have and as such could compromise or appear to compromise their decisions.

- A person, who is connected to the development, delivery or award of qualifications by the organisation, has interests in any other activity which have the potential to lead that person to act contrary to his or her interests in that development, delivery or award in accordance with the awarding organisations conditions of recognition.

- An informed and reasonable observer would conclude that either of the above situations was the case.

- Any individual or organisation working with a business that is in direct competition to Defence Security.

- Any individual having a close or familial relationship with a registered learner, or learners' family whilst being involved in decisions about the outcome of their accreditation or qualification or where the person whose remuneration is in part determined by the outcome of the assessment.

- A situation that may create the appearance of a conflict, or present a conflict of interest in connection with a person who has influence over the activities or finances of Defence Security.

Roles & Responsibilities

All relevant staff undertaking assessment ('assessors'), moderation ('moderators' or 'verifiers') and other individuals have a responsibility to be aware of the potential for a conflict of interest.

Such situations must be carefully managed to ensure that any conflict of interest does not detrimentally impact on the standards of Defence Security and its public confidence.

It is the duty of all individuals to disclose any actual or potential conflict of interest, to their line managers or the Director, in writing. The information submitted is then evaluated to identify if any further action is required and a written record of the outcome of the evaluation is kept and a copy will be provided to the concerned individuals.

If the individual concerned has any changes to their declared circumstances, they must inform their line manager immediately in writing, so that the conflict of interest can be evaluated, and the register updated.

Conflict Of Interest Policy

Purpose

The purpose of this policy is to provide guidance to relevant individuals and organisations on handling possible conflicts of interest that may arise at Defence Security.

This policy applies to all staff and other individuals whenever they interact or potentially interact with any of Defence Security's operations.

This Policy:

- Defines what is meant by conflict of interest sets out the roles and responsibilities for managing conflict of interest

- Illustrations of potential conflict of interest situations.

Scope:

It is the policy of Defence Security that each individual working within or acting on behalf of the company must be free from conflicts of interest that could adversely affect their judgement or objectivity to the organisation in conducting business activities and assignments.

Defence Security recognises that each individual working within or acting on behalf of the organisation may take part in legitimate financial, business, charitable and other activities outside of their recognised roles at Defence Security, but any potential conflict of interest raised by those activities must be acknowledged, disclosed, and in relevant cases properly managed.

It is the responsibility of each individual or organisation working within or acting on behalf of Defence Security to recognise situations in which they have a conflict of interest, or might reasonably be seen by others to have a conflict; to disclose this conflict and to take such further steps as may be appropriate and set out in more detail under the procedure below.

Definition of Conflict of Interest

A conflict of interest is a situation in which an individual, or organisation, has competing interests or loyalties. Conflicts of interest can arise in a variety of circumstances, and it is possible that people working alongside and/or for Defence Security may encounter potential conflicts of interest from time to time.

It is not possible to provide a definitive list of examples of conflicts of interest that could compromise the integrity of Defence Security.

However, the following situations could lead to perceived or actual conflicts of interest;

- When an individual has a position of authority in one organisation which conflicts with his or her interests in another organisation.

- When an individual has personal interests that conflict with his/her professional position at Defence Security.

- A conflict of interest may generally be defined as a conflict between the official responsibilities of a trainer, assessor, and internal verifier and any other interests the particular individual may have and as such could compromise or appear to compromise their decisions.

- A person, who is connected to the development, delivery or award of qualifications by the organisation, has interests in any other activity which have the potential to lead that person to act contrary to his or her interests in that development, delivery or award in accordance with the awarding organisations conditions of recognition.

- An informed and reasonable observer would conclude that either of the above situations was the case.

- Any individual or organisation working with a business that is in direct competition to Defence Security.

- Any individual having a close or familial relationship with a registered learner, or learners' family whilst being involved in decisions about the outcome of their accreditation or qualification or where the person whose remuneration is in part determined by the outcome of the assessment.

- A situation that may create the appearance of a conflict, or present a conflict of interest in connection with a person who has influence over the activities or finances of Defence Security.

Roles & Responsibilities

All relevant staff undertaking assessment ('assessors'), moderation ('moderators' or 'verifiers') and other individuals have a responsibility to be aware of the potential for a conflict of interest.

Such situations must be carefully managed to ensure that any conflict of interest does not detrimentally impact on the standards of Defence Security and its public confidence.

It is the duty of all individuals to disclose any actual or potential conflict of interest, to their line managers or the Director, in writing. The information submitted is then evaluated to identify if any further action is

required and a written record of the outcome of the evaluation is kept and a copy will be provided to the concerned individuals.

If the individual concerned has any changes to their declared circumstances, they must inform their line manager immediately in writing, so that the conflict of interest can be evaluated, and the register updated.

Review Due: April 2024

Equality and Diversity Policy

Defence Security is a progressive training organisation providing mandatory training to a range of organisations. We provide education and training and assessing qualifications through BIIAB.

At Defence Security we are committed to providing high quality training and qualifications, and to ensuring that equality of opportunity underpins all aspects of our work.

This policy relates to our commitment to equality and diversity in all aspects of our work.

It is important that all appeals/complaints are raised directly with Defence Security.

Our equality and diversity policy statement is set out below.

Policy statement

Defence Security recognises its responsibility to eliminate unlawful discrimination, challenge anti discriminatory practice, promote equality of opportunity and diversity in all aspects of its activities: as an employer and a provider of training and consultancy.

Defence Security is committed to promoting equal opportunity and to adopting proactive measures to address unlawful discrimination in the execution of its services.

Defence Security will ensure that equality of opportunity is prominent throughout our work; in making policy, managing the business, service delivery i.e. training, consultancy and assessment, in complying with current UK regulations, and in our employment practice.

Defence Security will provide a working environment that is free from any form of harassment, intimidation, victimisation or discrimination on the grounds of; nationality, race, colour, gender, sexual orientation, identity, ethnic or national origin, disability, marital status, gender reassignment, pregnancy, status or home responsibility, HIV or AIDS status, age, work status (part-time or fixed term), religious or political belief and socio-economic background. All individuals will be treated with dignity and respect and valued for who they are and for their contribution.

All Defence Security directors and staff are responsible for ensuring that the Equality and Diversity Policy is put into practice and that they have due regards to the need to:

i) challenge all forms of discrimination.
ii) eliminate unlawful discrimination.
iii) promote equality of opportunity.

Defence Security will review its Equality and Diversity Policy annually. The following opportunities are taken to invite feedback from staff, clients and students:

- Recruitment and Selection
- Initial Assessment
- Induction
- Assessment and Planning
- Learner Reviews
- Internal Verification
- External Verification
- Examinations
- Exit Interviews

This feedback will be included in the annual review of our policies.

Scope of Policy

Defence Security will adhere to all relevant Statutory Legislation and the Code of Practice as per Appendix 1.

In accordance with its commitment to equal opportunities, Defence Security will ensure that positive steps are taken to identify and combat all forms of discrimination so that no potential or existing members of staff, clients or students are discriminated against from any of the four main types of discrimination - Direct discrimination, Indirect discrimination, Harassment and Victimisation.

Direct discrimination is treating one person less favourably than others because of, for example their race, gender, sexuality or disability (a fuller list has been provided above).

Indirect discrimination is creating a condition, term of employment or requirement of service delivery which cannot be justified and which, in practise, prevents people from certain groups from receiving a service.

Defence Security will not tolerate any form of harassment when offensive or intimidating behaviour, or encouraging or allowing other people to do so, aims to humiliate, undermine or injure its target, causing any physical or mental harm.

Defence Security will not tolerate any form of Victimisation, which means treating somebody less favourably than others because they tried to make a discrimination complaint. Defence Security will ensure that we comply with the Public Interest Disclosure Act 1998, to ensure that all relevant protection is afforded to all relevant parties. This legislation is

“An Act to protect individuals who make certain disclosures of information in the public interest; to allow such individuals to bring action in respect of victimisation; and for connected purposes”

Defence Security recognises that the implementation of the Equal Opportunity Policy is vital

to its development and continuing success, and the Directors will take full and frank responsibility for ensuring effective implementation of the policy and code of practice.

We will ensure that all individuals and organisations which provide services for or on behalf of Defence Security, are aware of and fully complying with our commitment to equality of opportunity.

Defence Security will investigate any alleged breach of this policy by Directors, staff, clients or students. If the allegation is upheld, action will be taken which could result in disciplinary proceedings against the Directors, staff, clients or students, as detailed in our Maladministration and Malpractice Policy.

Aims of the Policy

- To comply with the general and specific duties of all UK Equal Opportunities Legislation.
- To fulfil our statutory obligation to raise awareness of the policy to all staff, clients and students.
- To ensure that all potential, new and existing staff, clients and students are informed of the policy and its implications. All students will be issued with a copy of the policy on registration, all job applicants will receive the policy when applying to work with us.
- To ensure that all students have access to a fair and well managed examination and assessment process, in accordance with both Defence Security and BIIAB guidelines for Maladministration and Malpractice.

Publishing Arrangements

Defence Security will ensure the policy statement is displayed and distributed throughout our business, in a variety of media, including but not limited to, paper copies issued at registration, the policy will be published online on the company's website.

Organisation, Consultation and Participation

As the employers, Defence Security Directors have the ultimate responsibility for ensuring compliance with Equal Opportunity Legislation.

The Directors shall carry out an annual review of the policies that are in use, ensuring the policies are up to date, reflect current good practice and legislation. We will consult as widely as possible with all stakeholders i.e. staff, training centres, students and any other relevant parties.

Equal Opportunities: Functional Responsibilities

The Directors are responsible for:

i. personnel related policies and strategies.
ii. developing and delivering a programme of (or arranging delivery of) staff development in all aspects of diversity and equality of opportunity matters.
iii. advising and supporting staff to identify and disseminate good equal opportunity practice, particularly in relation to equal treatment in all aspects of the staff and client and student experience.
iv. ensuring that all HR policies and procedures meet legal and ethical standards in relation to equal opportunity.
v. advising staff on procedures in relation to the Defence Security Equal Opportunities Policy.

Making an Equal Opportunities Complaint

An employee or service user who feels they have not been fairly treated within the scope of this policy should raise the matter through Defence Security's Grievance and Disciplinary Procedure.

Dealing with discrimination and harassment as an Training Provider

As a Training Provider Defence Security complies with anti-discrimination and human rights legislation and promotes the wellbeing of candidates. Defence Security actively seek to eliminate all forms of discrimination and harassment – whether towards candidates or staff. We will use the following model for challenging discrimination:

- Recognising individualism and value difference.
- Breaking down stereotypes.
- Challenging discrimination.
- Role modelling appropriate behaviour.

In general, this is dealt with through our own disciplinary policy, but in all circumstances the safety, well-being and support needs of the victim is our first priority.

Defence Security will comply with its legal responsibility to make a written record of any racist incident which takes place on our premises or any satellite office.

Certain racist incidents may also be criminal offences in England and Wales under the Crime & Disorder Act 1998. These include:
i) Racially aggravated assaults, including common assault, actual bodily harm, and grievous bodily harm and wounding.
ii) Racially aggravated criminal damage, including racist graffiti, damage to property and arson (lighting fires).
iii) Racially aggravated public order/harassment, including engaging in behaviour which causes (or is likely to cause) harassment, distress or fear of violence.

The police, not Defence Security, are responsible for investigating and dealing with any racist incidents where criminal offences may have been committed. All racist incidents of this kind will be reported to the police as soon as possible.

Defence Security will also report the incident to the police if asked to do so by the victim or their parents.

In addition to the general principles for dealing with discrimination or harassment, Defence Security will adhere to the specific rules which exist for dealing with sexual harassment and discrimination. If the perpetrator is an employee of Defence Security or other professional in a position of authority, then this will normally be either a criminal matter (in which case it should be referred to the police) or a disciplinary offence under Defence Security's Disciplinary Procedure.

This policy was approved by: Abdul Basit, April 2022

Review Due: April 2024

APPENDIX 1

The relevant Acts of Parliament relating to equal opportunities policy are:

- Rehabilitation of Offenders Act 1974.
- The Public Order Act 1986.
- Employment Act 1989.
- Human Rights Act 1998.
- The Public Interest Disclosure Act 1998.
- Protection from Harassment Act 1997.
- Part Time Worker Regulations 2000.
- The Race Relations (Amendment) Act 2000.
- The Gender Recognition Act 2004.
- Racial and Religious Hatred Act 2006.
- Equality Act 2010

In addition, Defence Security will comply with the following codes of practice relating to equal opportunities; including guidance available from:

- Equality and Human Rights Commission
- Disability Rights Commission.
- ACAS : Advisory Conciliation and Arbitration Service.
- Equality Act Codes of Practise

The Equality Act Codes of Practise can be found at: www.equalityhumanrights.com

The full details of the Equality Act 2010 can be found at: www.legislation.gov.uk

This policy was approved by: Abdul Basit, March 2022

Review Due: March 2024

Examination Invigilation Policy

Our aim:
Defence Security is committed to providing a quality service for its staff and service users and working in an open and accountable way that builds the trust and respect of all our stakeholders.

Our responsibility:
Ideally learners will be registered by the relevant member of Centre staff no later than at commencement of the course; however, this is often not possible, and learners should be registered on the relevant qualification as soon as possible thereafter.

Defence Security has the responsibility to take all reasonable steps to confirm the identity of the learners and they do this by requesting sufficient personal data to complete the registration form and inputting a unique learner number (ULN) –if the learner opts to have a ULN – to ensure the learner can be clearly and uniquely identified.

Defence Security will nominate personnel who will be authorised to check and submit course registration/certification requests. Defence Security is responsible for ensuring that the course has been delivered effectively; the learner has completed the relevant parts of the course and the identification of the learner has been confirmed.

In addition, they will check course paperwork and registration requests and certificate claims to ensure they have been fully and correctly completed, including:

- That result information match course registration details.
- Only appropriately competent trainers, assessors and verifiers were involved in the delivery/assessment.
- The correct documentation was used.
- Learner details are correctly completed.
- Investigating any suspicious entries or reasons for omissions of key data, resolving any issues with the relevant trainer, assessor and/or internal verifier and when required raising the matter with the Awarding Organisation.

Any completed Examination Answer Sheets will also be checked by the Centre to ensure full and clear completion and that the correct qualification has been listed, as well as being signed off by a suitable, empowered and authorised member of staff.

The initial trigger for all certificate claims rests with Defence Security.
Only when we are satisfied that a learner has completed the relevant assessments and have reached the specified level of attainment for the qualification will Defence Security make a claim for certification to claim the full qualification.

Learner Information:
Defence Security will make it clear to the learners well in advance of the examination, that they should notify the Centre, should they require Reasonable Adjustments and/or Special Consideration.

Awarding Organisations policies in respect of Reasonable Adjustments and Special Consideration will be complied with.

Learners may be instructed to bring identification to the assessment for checking by the invigilator. This instruction should be given ahead of the course/assessment when the learner registers and/or with any pre-course materials.

Invigilators:
The invigilator must not be related to learners. It is our responsibility to ensure that the invigilator is suitable to invigilate examinations.

Examination Procedures:
Prior to the examination, Invigilators/Assessors responsibilities include:

- Inspecting the examination room to ensure that the accommodation is suitable, and the seating is arranged in such a way to avoid malpractice;
- Ensure that there is an 'Exam in Progress' sign visible on any entry door to the examination room;
- Ensure that all learning aids (such as workbooks, wall posters etc.) that may assist learners with the examination are covered or removed;
- Verify that all learners are present;
- Identify any individuals for whom special arrangements have been approved.
- Familiarise themselves with the Examination and Invigilators Procedures;
- Explain evacuation arrangements to learners, in the event of an emergency;
- Explain evacuation arrangements to learners, in the event of an emergency;
- Be confident that all the individuals attempting to take the examination are who they say they are;
- Ensure all learners add their details to the Learner List.

Examinations:
Prior to the examination, Invigilators/Assessors responsibilities are to:

- Arrive at the examination location in good time.
- Inform the learners of the correct Centre and Trainer Number.
- Inform the learners of the start and finishing time of the examination, referring to a clock that should be visible to all learners.
- Ensure that all learners are positioned sufficiently apart to avoid the risk of malpractice, 1.5 metres is the recommended distance between learners.
- Inform learners that they are not permitted to refer to any materials other than a standard dictionary. Invigilators/Assessors should check that only authorised materials are on the learner's desks.
- If a paper-based assessment, inform learners that multi-media devices, such as mobile phones, tablets, smart watches, need to be turned off and not placed on the examination desk.
- Inform all learners that they should read all instructions on the examination paper before answering the questions.
- Inform all learners that they are prohibited from communicating with other learners during the examination and that the Invigilator/Assessor is not permitted to provide any further explanation or guidance on examination questions.
- Once the learners are settled, ensure that the learners have the correct examination paper, noting the title of the examination.

The Invigilators responsibilities are to ensure learners are supervised throughout the examination.

Absolute silence must be maintained throughout the examination.

Learners who arrive after the starting time for an examination may, at the discretion of the Invigilator/Assessor, enter the room and sit the examination providing that they do not disturb the other learners. They must, however, finish the examination at the same time as the other learners.

Learners who need to leave the examination room must be accompanied by an Invigilator/Assessor, who must ensure that they do not speak to anyone else, make a telephone call or refer to any notes.

If an Invigilator/Assessor observes or suspects a learner of malpractice, that learner should be asked to stop. Should the action be considered serious enough, a learner's examination paper and answer sheet should be collected, and the learner asked to leave the examination room.

Invigilators are expected to remind the learners of the time remaining approximately 15 minutes before the end of the examination.

In the event of an emergency, the Invigilator/Assessor should evacuate the examination venue in accordance with venue procedures. All examination papers and answer sheets must be left on the learners' desks.

If an Invigilator/Assessor is satisfied that the integrity of the examination has not been compromised, the examination can be resumed for the remaining allocated time.

Policy review date**:** April 2024

Health and Safety Policy

Defence Security is a progressive training organisation providing mandatory training to a range of organisations. We provide education and training and assessing qualifications through BIIAB.

At Defence Security we are committed to providing high quality training and qualifications, and ensuring that equality of opportunity underpins all aspects of our work.

This policy relates to our health and safety and covers all aspects of our work

Our health and safety policy statement is set out below.

Policy statement

Defence Security recognises its responsibility to eliminate unnecessary risk and hazard through the course of running our business whose primary aim is to provide mandatory training courses, we shall promote a safe working and training environment at all times.

We shall ensure that all staff, students and visitors to our premises whether wholly owned, leased or hired for training courses shall be as far as is practicable, safe from first arriving on site to leaving the site.

We shall aim to achieve compliance with all local, national and European legislation through excellent occupational health and safety performance.

Defence Security will provide adequate resources to implement this policy and any supporting policies.

Defence Security will establish and maintain a safe and healthy working environment and risk assessments shall be recorded and reviewed on a regular basis. The risk assessments shall cover:

- General risk assessments on premises, equipment, and work stations.
- Activity based risk assessments, on all training activities.
- Manual handling assessments on all lifting and handling associated tasks.
- COSHH assessments on all chemicals used throughout the business.
- Fire risk assessments.
- Individual risk assessments for any staff member of student who needs adaptions making to enable them to carry out the course or their employment.

These risk assessment will ensure that significant risks arising from our work activities under our control are eliminated or adequately controlled.

Defence Security will develop and implement appropriate occupational health and safety procedures, and safe working protocols.
We have included health and safety as a responsibility for all managers, trainers and assessors.

All staff will be required to read and sign to say they have understood this policy statement; the signed form will be kept in their staff personnel file. Students will be referred to a copy of our policy at registration, and as with all of our policies they will be available on our website.

Defence Security will review its Health and Safety Policy every two years. The following opportunities are taken to invite feedback from staff, clients and students:

- Recruitment and Selection
- Initial Assessment
- Induction
- Assessment and Planning
- Learner Reviews
- Internal Verification
- External Verification
- Examinations
- Exit Interviews

This feedback will be included in the annual review of our policies.

This policy was approved by: Abdul Basit, April 2022

Review Due: April 2024

Learner Identification Policy

This Policy establishes guidelines for the process of validating learner identity and authenticating learner evidence. The process begins with initial provision of approved forms of identification for the purpose of enrolment on the qualification, progresses through stages of validating assessment, and concludes with submission of authentic Learner work.

It is vital that all learners are the ones completing the assessment/examinations. This policy states the procedures that have been put in place to establish that the learner is the person who participates in, completes the qualification and receives the award of certificate. All learners are affected by this policy. It is Defence Security's responsibility to ensure that the checks detailed in this policy are carried out.

Definitions

Identity fraud: Any learner who allows another person to impersonate them or in any other way commit identity fraud in any course, exam or other academic exercise will be dismissed from the course. This also applies to a learner who is found to impersonate another.

Policy Authenticating Learner identity is integral:

- To prevent impersonation of learners on the qualification and to protect and uphold the integrity and reliability of the qualification. Defence Security must confirm they have seen valid proof of identification.

- When authenticating previous qualifications for RPL (Recognition of Prior Learning) certificates or other evidence of previous qualifications must be an accurate reflection of a learner's achievements.

- To maintain credibility: through certificates, diplomas and certified forms, Defence Security must declare that a Learner named on these documents has personally achieved all relevant academic requirements. Qualifications are at risk if Learners emerge as having achieved academically but have not acquired new and relevant knowledge or skills.

- To ensure learner achievement. Training Providers have a responsibility to their learners to facilitate learning and prepare individuals for the challenges in their qualification. This can only occur if the learner has successfully completed the course and achieved learning at the relevant standard of achievement.

Areas of concern

There are two main areas of concern where authentication of learner identification needs to be addressed:

- Plagiarism and cheating - it is necessary to determine if the work from a learner is authentic and unique. Details of identifying and dealing with instances of plagiarism are addressed in the Malpractice and Maladministration Policy.

- Impersonation – it is necessary to determine if the learner receiving the award of certificate is the person completing the evidence.

Learners have responsibility to provide appropriate evidence of identity. Defence Security has responsibility for upholding the validity of the qualification and that all staff members fully meet the requirements set out in this policy. Defence Security is responsible for obtaining the necessary evidence and carry out the checks required as per the procedure below.

Procedures

Defence Security has several procedures to ensure that a Learner who gains an award for academic achievement is the person who completes the work.

Authentication is demonstrated by the following:

- All learners must provide supporting evidence of personal identification prior to the commencement of study in the form of photographic ID. Valid examples are current Passport or Photo ID driving licence. It is the Training Provider's responsibility to obtain, record and save this evidence either on an electronic system or manually but all data should meet the GDPR and Data Protection Act. Failure to obtain this evidence prior to the Learner commencing the qualification will constitute malpractice of the process and sanctions may be given to the Defence Security.

- Evidence of name change i.e. copies of marriage certificate and a copy of a recent utility bill (within 3 months) as proof of name and address.

- Learners must provide copies of all previously certificated qualifications in any request of RPL.

- Each evidence submission must include a signed declaration confirming that all the work being submitted is the Learner's own work. This signature will be compared to ID signatures.

Defence Security implement a variety of assessment methods and trainers have a right to question the content or meaning of any submitted assignments with the learner, to verify that a verbal level of understanding reflects the written content. Defence Security operates a zero-tolerance approach where a learner who has registered as a learner is not the person completing the work.

Any proven instances will result in the Learner being disqualified and removed from the qualification instantly or risk the award of certificate being withdrawn. All evidence must be recorded by the Trainer/Internal Quality Assurer.

Policy review date: April 2024

Maladministration and Malpractice Policy

Defence Security is a progressive training organisation providing mandatory training to a range of organisations. We provide education and training and assessing qualifications through BIIAB.

At Defence Security we are committed to providing high quality training and qualifications, and to ensuring that equality of opportunity underpins all aspects of our work. This policy relates to maladministration and malpractice and covers all of our staff and students; this document sets out our formal procedure for dealing with such incidents.

Defence Security will strive to ensure that all work carried out by our staff, training centres and contractors is of the highest quality.

Defence Security Management and Staff aim to provide a high standard of service to all learners, so that they have the opportunity to develop to the fullest of their potential. Quality is at the heart of everything we do, it is vital that all of our learners receive the highest standard of training, and that our examinations are both valid and held up as an example of good practice within the wider training sector, therefore it is essential that our policies are both rigorous and thorough.

We have policies, procedures, protocols, work systems and instructions in place to ensure that all of our work is of the highest standard at all times, therefore any allegations of Maladministration within the business side or the examinations and assessment side will be treated with the respect and urgency they deserve.

Definition of Maladministration

> *Maladministration is essentially any activity or practice which results in noncompliance with administrative regulations and requirements and includes the application of persistent mistakes or poor administration within a centre (eg inappropriate learner records).*

Definition of Malpractice

> *Malpractice is essentially any activity or practice which deliberately contravenes regulations and compromises the integrity of the development, delivery, internal or external assessment process and/or the award of any of the qualifications we offer.*

Malpractice could involve centre staff, learners, external verifiers and awarding organisation staff or contractors.

For the purpose of this policy the terms maladministration and malpractice also cover misconduct and forms of unnecessary discrimination or bias towards learner(s). Defence Security has policies and procedures in place to minimise the possibility of malpractice or maladministration occurring within the centre. In particular, qualifications have to be delivered according to a specified process, all staff and contractors' work is subject to quality assurance, and both paper-based and IT administration is carried out according to specified procedures.

The categories listed below are examples of centre and learner malpractice. Please note that these examples are not exhaustive and are only intended as guidance on our definition of malpractice:

- Contravention of our centre and any qualification approval conditions
- Denial of access to resources (premises, records, information, learners and staff) when requested by any authorised awarding body representative and/or the regulators
- Failure to carry out delivery, internal assessment, internal moderation or internal verification in accordance with awarding body requirements
- Deliberate failure to adhere to our learner registration and certification procedures
- Deliberate or persistent failure to adhere to our centre recognition
- Deliberate failure to maintain appropriate auditable records, eg certification claims, starter, leaver and evaluation records
- Persistent instances of maladministration within the centre, by staff, trainers, assessors, internal verifiers or contractors
- Fraudulent claim for certificates
- The unauthorised use of inappropriate materials / equipment in assessment settings (eg: mobile phones)
- Staff intentionally withholding information from Defence Security Management which is critical to maintaining the rigour of quality assurance and standards both the centre and of the qualifications we deliver
- Deliberate misuse of logo and trademarks or misrepresentation of a training centres relationship with Defence Security
- Forgery of evidence
- Collusion or permitting collusion in exams
- Trainers allowing learners to still be working towards a qualification after certification claims have been made
- Contravention by our training centres, trainers, assessors, Internal Verifiers and learners of the assessment arrangements we specify for our qualifications
- Insecure storage of assessment materials and exam papers issued by any awarding body
- Plagiarism of any nature by learners

- Unauthorised amendment, copying or distributing of exam papers issued by any awarding body
- Inappropriate assistance to learners by centre staff (eg unfairly helping them to pass a unit or qualification)
- Submission of false information to gain a qualification or unit
- Deliberate failure to adhere to the requirements of our policies.
- Conduct during assessment

Defence Security will treat all allegations of Maladministration and Malpractice as a serious incident and will launch a full investigation and where appropriate suspend staff, trainers, assessors, internal verifiers or students.

All awarding bodies that we are registered with will be informed of the allegations and the outcome of our investigation. We will comply with any external investigations that are required by the examining organisations or any regulatory authorities, including Police investigations as appropriate.

In the event of serious Maladministration or Malpractice, such as fraudulent activity, theft, dishonesty, corruption and abuse, the issue will be referred to the police for a full criminal investigation.

Police Station: Newtown Police Station

Address: 262
Summer Lane
Birmingham
B19 2QG

Telephone: 101

All staff and students will be able to appeal any sanctions imposed using either the assessment appeals procedure or the employee grievance procedure.

Confidentiality and whistleblowing

Whistleblowing is a term used to refer to an individual who discloses information relating to actual malpractice or maladministration and/or the covering up of such practices. The malpractice or maladministration is often committed by the individual's employer, although this is not necessarily the case. Whistleblowers have protection in law under the Public Interest Disclosure Act in certain circumstances.

Ofqual has published guidance on this which can be found at:

http://www.ofqual.gov.uk/files/2011-10-31-ofqual-whistleblowing-policy.pdf

In this guidance, Ofqual states that centre staff who wish to make a whistleblowing disclosure to someone outside their organisation should normally do so to the relevant awarding organisation.

If the issue is about the awarding organisation itself, the disclosure should be directly to Ofqual.

Qfqual contact details:

Office of Qualifications and Examinations Regulation
Earlsdon Park
53-55 Butts Road
Coventry
CV1 3BH
United Kingdom

Switchboard: 0300 303 3344
(Lines are open Monday to Friday, 9.00am to 5.00pm)

Textphone: 0300 303 3345

Fax: 0300 303 3348

Email: info@ofqual.gov.uk

Defence Security will always endeavour to keep a whistleblower's identity confidential where asked to do so, although we cannot guarantee this and we may need to disclose your identity to the police or other law enforcement agencies, the courts or another person to whom we are required by law to disclose your identity. A whistleblower should also recognise that he or she may be identifiable by others due to the nature or circumstances of the disclosure.

While we will consider investigating issues which are reported to us anonymously, we shall always try to confirm an allegation by means of a separate investigation before taking up the matter with those to whom the allegation relates. It is not always possible to investigate or substantiate anonymous disclosures.

Defence Security will make every effort to ensure that all of our staff, including management, administrators, trainers, assessors and internal verifiers and all learners follow all the requirements of our training centre and the awarding bodies.

All staff will be required to read this policy and sign to say that they have read and understood the policy. These signatures will be kept in the staff members personnel file.

This policy was approved by: Abdul Basit, March 2022

Review Due: March 2024

Privacy & Cookie Policy

Document Specification:			
Purpose:	To set out Defence Security approach to ensuring the Privacy of individuals and the use of Cookies on its websites, etc., in line with the GDPR		
Accountability:	Defence Security	Responsibility:	Defence Security
Last Review date:	April 2022	Next Review due:	April 2024
Version:	1	Law/Regulations covered:	Policy & Electronic Communications Regulations (amended 2016) General Data Protection Regulations Data Protection Bill 2018

Defence Security
St Georges Community Hub
Great Hampton Row
Birmingham
B19 3JG

Tel: 0121 448 1661
Email: basit@defence-security.co.uk
Website: www.defence-security.co.uk

CONTENTS

1. Overview

This Policy covers the data collected and processed by Defence Security who can be contacted at:

Defence Security
St Georges Community Hub
Great Hampton Row
Birmingham
B19 3JG
Tel: 0121 448 1661

Defence Security is the Data Controller of the personal data we process on our own behalf and the Data Processor of data processed on behalf of our clients. We have a legal duty to protect the privacy of all, personal and business data obtained from you while you are using our website, as well as in the provision of our services to you. This Privacy Policy explains what information we may collect from you and the purposes for which it will be used. This Policy complies with all current data protection and privacy regulations in the UK, including, but not limited to, the General Data Protection Regulations (the GDPR) and the Privacy and Electronic Communications Regulations (the PECR).

The GDPR relates to 'personal data' which covers any information which makes an individual (the Data Subject) identifiable.

2. Purpose of and Legal Basis for Processing Personal Data

Defence Security will only process personal data for the purposes of delivering the services contracted by our clients, unless we are provided with specific consent to process for other purposes, such as marketing, or the purpose of complying with local laws or regulations. Personal data will never be processed without the knowledge and/or permission of the Data Subject.

Where you have contracted for us to provide a regulated qualification, we will be sharing your information with the recognised Awarding Organisation, as required by the applicable Regulator(s) as part of our legal obligation.

By using our services, including accessing our website and the forms, etc. therein, you give your agreement to our processing any personal data we may have as described in this policy.

3. Types of Personal Data Processed

Personal Data is any information which could potentially make an individual identifiable and can include, but may not be limited to, your name, address, date of birth, email address and IP address.

We collect data in a number of ways including, but not necessarily limited to:

- Contact forms on our website completed and submitted by a Data Subject
- As part of a Contract for Services, i.e. names and contact information of individuals, including where they are acting on behalf of a client company
- Provided to us by clients in order that we can deliver the services they have contracted us for

Our contact forms make it clear that the information will be used for the purposes of the contact (e.g. to respond to a query or provide a quote, etc.) but also provide the option for consent to expand the processing of that data for marketing purposes. Similarly, any contract for services will set out what the personal data will be used for.

Personal Data provided to us by our clients as part of our service provision will be processed only in accordance with the contract for services and no such data will be used for the benefit of Defence Security.

4. Our Website and Cookies

4.1. Who manages our website?

The content of our website is owned and edited by the Defence Security.

4.2. Website usage information

Web usage information is collected by our web server and from other sources including page tagging techniques using JavaScript and cookies. We use cookies to analyse website usage trends, understand user journeys and gather broad demographic information for aggregate use. Our cookies are not linked to personally identifiable information and we do not collect, store or process the IP addresses of visitors browsing our website.

The type of website usage information that we collect during your visits to our site includes, for example, the date and time, pages viewed or searched for, publications ordered, guides printed, tools used, subscriptions and referrals made, some truncated postcode or telephone area code information entered on forms (which is not traceable back to you) and other information relating to your usage of our website.

Where you are a registered user of our website and have logged in, we may collect web usage information to enable us to build a demographic profile or to improve the services you have requested from us.

We may also use web usage information to create statistical data regarding the use of our website and we may then use or disclose that statistical data to others for marketing and strategic development purposes, however, no individual identities will or can be identified in such statistical data.

4.3. Cookies

Cookies are small pieces of data given to your browser by a website which may be stored as text files in the cookie directory of your computer. Cookies are not programs and cannot collect information from your computer. They do not damage your computer and are defined as "a piece of text stored on a user's computer by their web browser. A cookie can be used for authentication, storing site preferences, shopping cart contents, the identifier for a server-based session, or anything else that can be accomplished through storing text data" (source: Wikipedia, 2011).

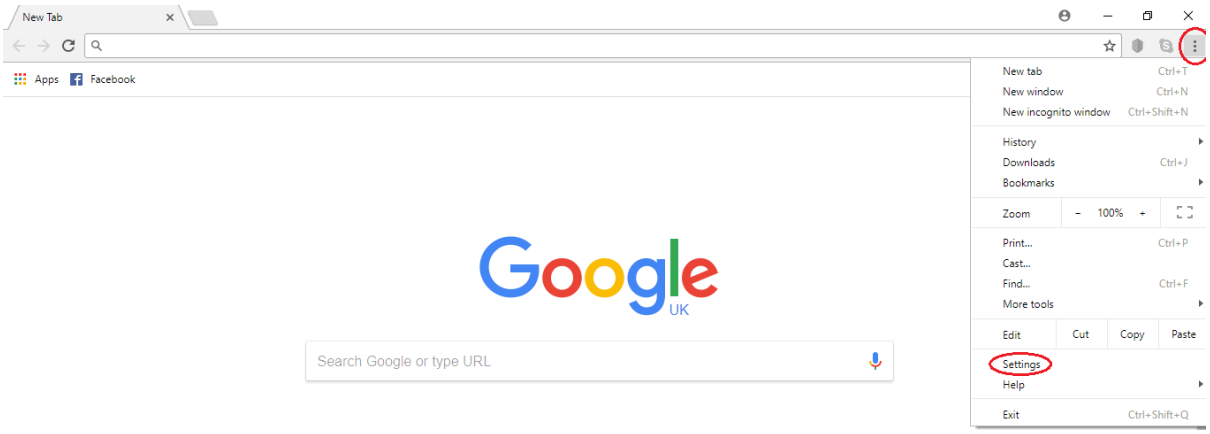
Each website may send cookie data to your browser which may save it if your browser's preferences allow it to do so. To protect your privacy your browser only returns a cookie to the website that sent you the cookie and does not send it to any other website. A website cannot access your cookie directory or information on your computer, instead relevant cookies are included by your browser within each request you make to the website. A website can only obtain cookie data that your browser sends to it.

You do not have to accept cookies and you can change the settings within your browser to accept all cookies, reject all cookies, reject cookies from certain websites, notify you if a site is requesting to set a cookie, and set various other options. Please see below in '4.4 Further information about cookies' for more details on how you might do this.

Switching off cookies will still allow you to view the majority of content on our site, however, it will prevent you logging in and so accessing personalised information. It will also stop us remembering your login User ID, if you ask us to do so, and may restrict your use of our interactive tools and of some services available through linked sites.

4.4. Further information about cookies

If you would like to opt out of, or restrict the use of cookies when visiting our, or any other third party's website, you are able to adjust the settings in your Internet browser to do this. Exactly how this is done will depend on which browser you use for access to the Internet. Each browser has its own variation on how this can be achieved, but it is usually under 'Settings' which can be found at the end of the Search bar, e.g. on Chrome it is found as follows:



You then need to go to "Advanced", then "Privacy and Security", then "Content Settings" and "Cookies" and choose the most appropriate setting for yourself.

Users should check their Internet browser for details of how to amend, remove or restrict the use of cookies on their computer, tablet or other internet enabled device.

For further information about cookies, please refer to:

- Find information on internet browser cookies on the Information Commissioner's website

4.5 Third party content and linking to other websites

This privacy policy applies only to our website. We are not responsible for privacy practices within any other websites. You should always be aware of this when you leave our website and we encourage you to read the privacy statement on any other website that you visit. We embed external content from third-party websites such as YouTube, Twitter and LinkedIn including cookies. This content is not published on our website. It is delivered using devices and services from third party sites that can be inserted into our site such as media players, RSS feeds and widgets. These websites may use cookies. Their content is subject to the privacy policy of the relevant third-party provider and not ours.

5. Information sharing and disclosure

We may share your data with specified third parties for the purposes of supplying the services you have contracted us for or if required to by law or by a regulation based on a law. We will not sell, rent or disclose your information to any third parties other than those set out in this privacy policy without your prior consent.

We do not transfer your personal data outside of the UK and the European Economic Area.

Or

We may transfer your personal data outside of the UK for the purposes of backing upto a cloud server hosted by Defence Services who are based St Georges Community Hub, Great Hampton Row, B19 3JG, Birmingham, United Kingdom however your personal data is kept encrypted at all times so that it cannot be read by the service provider. All personal data is still under the remit of the GDPR, regardless of our use of storage outside the UK and the EEA.

6. Retention of Data

Personal Data will always be held for the minimum amount of time required. This will depend on a number of factors, such as the terms and length of a contract or a relevant law or regulation based on law. It will be deleted a maximum of 3 years after such a period has ended under our semi-annual data clearance procedures. Personal Data that has been gathered via our website contact forms will be held for a maximum of 3 years after the initial contact, unless additional permission is obtained from the Data Subject or a contract for services is brought into force in the interim.

Electronic Personal Data is encrypted and held in a secure manner on physical and cloud-based services. The encryption used meets all current requirements for encrypted services and is updated regularly to ensure that it remains fit for purpose. Electronic data is deleted following a secure process to ensure there is no lapse in security at the point of deletion.

Paper based Personal Data is held in secure, fire-proof, locked cabinets. It is destroyed under contract with a secure data destruction company.

7. Your Rights

Under current legislation, Data Subjects have the following rights:

- **To be informed** – This policy is one of ways in which Defence Security informs you how and why we process your data
- **Of Access –** All Data Subjects have the right to quest access to all of the data we hold on them. Any Data Subject requests received will be reviewed and responded to within one calendar month of receipt of the request. Most requests will be fulfilled free of charge, however, Defence Security reserves the right to charge a reasonable administration fee for any requests deemed to be excessive, unfounded or repetitive.
- **Of rectification –** Should you find that any data we hold about you is incorrect, you can ask us to correct it and we will investigate and respond within one calendar month of receipt of the request.
- **Of Erasure –** You can ask for your Personal Data to be erased permanently. All such requests will be responded to within one calendar month of the receipt of a request. Please note that, whilst we will always endeavour to fulfil requests, there may be some instances where this is not possible due to legal or regulatory reasons. We will always provide a full explanation in any such instances.
- **To restrict processing –** If you do not wish for your data to be erased, you may ask for it to be restricted so that we continue to hold it but not process it or use it in any way – we would essentially 'archive' your data. This is only applicable in certain circumstances, however we will look at all requests and respond within one calendar month of the receipt of a request.
- **To data portability –** All electronically held data can be transferred to another company in a structured, commonly used and machine readable format on request. Please note that this will only include the data you have provided to us and not any ancillary data produced as a result of the services we have created during the provision of our services or where that data includes information regarding a third party. All requests for moving data will be responded to within one calendar month of a request being received.
- **To Object –** You can object to our processing data for the purposes of marketing, scientific/ historical research and statistics, or legitimate interests or in the performing of a task in the public interest /exercise of official authority (including profiling). All such requests shall be responded to within one calendar month
- **Rights related to automated decision making, including profiling –** The GDPR sets out specific rights in relation to automated decision making. Please note that Defence Security does not use any form of automated decision making system whilst processing your data.
- **To complain –** You have the right to raise a complaint regarding the processing of your data or our response to a request under the above rights. As part of this, you also have the right to escalate your complaint to a supervisory authority. In respect of data handling, you have the right to escalate your complaint to the Information Commissioner's Office (ICO). Please go to https://ico.org.uk/for-the-public/raising-concerns/ for full details.

Data Subjects have the right to withdraw their consent to our processing their data at any time.

In respect of any of the rights indicated above, if you would like to make a request, require further information, or have a complaint regarding our processing of your data please contact us at:

Email: basit@defence-security.co.uk

Website: www.defence-security.co.uk

Address: Defence Security
St Georges Community Hub
Great Hampton Row
Birmingham

B193JG

Telephone: 0121 448 81661

8. Changes to this policy

We may make changes to this privacy policy at any time. Changes will be posted on our website and are effective immediately, except where they relate directly to a contract for services where all changes will be subject to the agreements in that contract. Regularly reviewing this Policy ensures that you are always aware of what information we collect, how we use it and under what circumstances, if any, we will share it with other parties.

Privacy & Cookie Policy

Document Specification:			
Purpose:	To set out Defence Security approach to ensuring the Privacy of individuals and the use of Cookies on its websites, etc., in line with the GDPR		
Accountability:	Defence Security	Responsibility:	Defence Security
Last Review date:	April 2022	Next Review due:	April 2024
Version:	1	Law/Regulations covered:	Policy & Electronic Communications Regulations (amended 2016) General Data Protection Regulations Data Protection Bill 2018

Defence Security
St Georges Community Hub
Great Hampton Row
Birmingham
B19 3JG

Tel: 0121 448 1661
Email: basit@defence-security.co.uk
Website: www.defence-security.co.uk

CONTENTS

1. Overview

This Policy covers the data collected and processed by Defence Security who can be contacted at:

Defence Security
St Georges Community Hub
Great Hampton Row
Birmingham
B19 3JG
Tel: 0121 448 1661

Defence Security is the Data Controller of the personal data we process on our own behalf and the Data Processor of data processed on behalf of our clients. We have a legal duty to protect the privacy of all, personal and business data obtained from you while you are using our website, as well as in the provision of our services to you. This Privacy Policy explains what information we may collect from you and the purposes for which it will be used. This Policy complies with all current data protection and privacy regulations in the UK, including, but not limited to, the General Data Protection Regulations (the GDPR) and the Privacy and Electronic Communications Regulations (the PECR).

The GDPR relates to 'personal data' which covers any information which makes an individual (the Data Subject) identifiable.

2. Purpose of and Legal Basis for Processing Personal Data

Defence Security will only process personal data for the purposes of delivering the services contracted by our clients, unless we are provided with specific consent to process for other purposes, such as marketing, or the purpose of complying with local laws or regulations. Personal data will never be processed without the knowledge and/or permission of the Data Subject.

Where you have contracted for us to provide a regulated qualification, we will be sharing your information with the recognised Awarding Organisation, as required by the applicable Regulator(s) as part of our legal obligation.

By using our services, including accessing our website and the forms, etc. therein, you give your agreement to our processing any personal data we may have as described in this policy.

3. Types of Personal Data Processed

Personal Data is any information which could potentially make an individual identifiable and can include, but may not be limited to, your name, address, date of birth, email address and IP address.

We collect data in a number of ways including, but not necessarily limited to:

- Contact forms on our website completed and submitted by a Data Subject
- As part of a Contract for Services, i.e. names and contact information of individuals, including where they are acting on behalf of a client company
- Provided to us by clients in order that we can deliver the services they have contracted us for

Our contact forms make it clear that the information will be used for the purposes of the contact (e.g. to respond to a query or provide a quote, etc.) but also provide the option for consent to expand the processing of that data for marketing purposes. Similarly, any contract for services will set out what the personal data will be used for.

Personal Data provided to us by our clients as part of our service provision will be processed only in accordance with the contract for services and no such data will be used for the benefit of Defence Security.

4. Our Website and Cookies

4.1. Who manages our website?

The content of our website is owned and edited by the Defence Security.

4.2. Website usage information

Web usage information is collected by our web server and from other sources including page tagging techniques using JavaScript and cookies. We use cookies to analyse website usage trends, understand user journeys and gather broad demographic information for aggregate use. Our cookies are not linked to personally identifiable information and we do not collect, store or process the IP addresses of visitors browsing our website.

The type of website usage information that we collect during your visits to our site includes, for example, the date and time, pages viewed or searched for, publications ordered, guides printed, tools used, subscriptions and referrals made, some truncated postcode or telephone area code information entered on forms (which is not traceable back to you) and other information relating to your usage of our website.

Where you are a registered user of our website and have logged in, we may collect web usage information to enable us to build a demographic profile or to improve the services you have requested from us.

We may also use web usage information to create statistical data regarding the use of our website and we may then use or disclose that statistical data to others for marketing and strategic development purposes, however, no individual identities will or can be identified in such statistical data.

4.3. The Use of Cookies

Cookies are small pieces of data given to your browser by a website which may be stored as text files in the cookie directory of your computer. Cookies are not programs and cannot collect information from your computer. They do not damage your computer and are defined as "a piece of text stored on a user's computer by their web browser. A cookie can be used for authentication, storing site preferences, shopping cart contents, the identifier for a server-based session, or anything else that can be accomplished through storing text data" (source: Wikipedia, 2011).

Each website may send cookie data to your browser which may save it if your browser's preferences allow it to do so. To protect your privacy your browser only returns a cookie to the website that sent you the cookie and does not send it to any other website. A website cannot access your cookie directory or information on your computer, instead relevant cookies are included by your browser

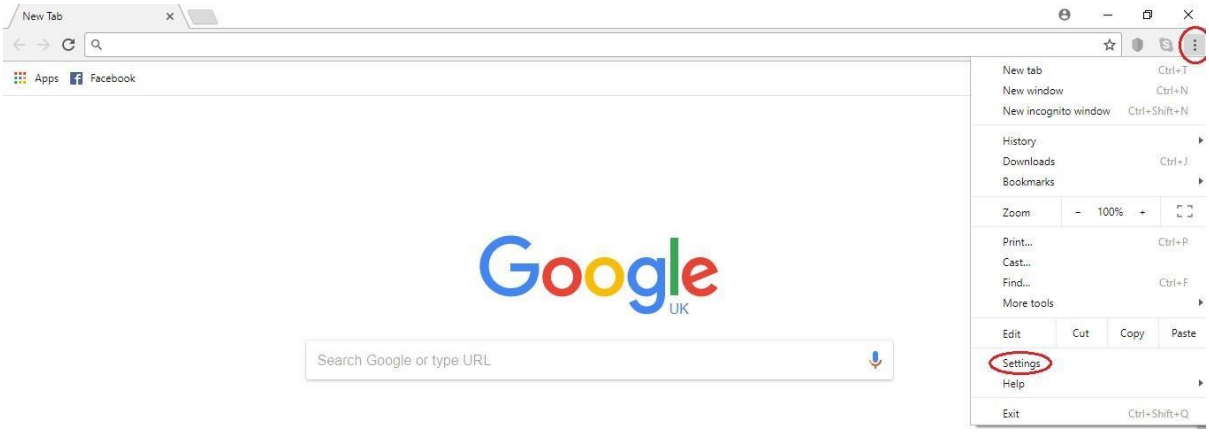
within each request you make to the website. A website can only obtain cookie data that your browser sends to it.

You do not have to accept cookies and you can change the settings within your browser to accept all cookies, reject all cookies, reject cookies from certain websites, notify you if a site is requesting to set a cookie, and set various other options. Please see below in '4.4 Further information about cookies' for more details on how you might do this.

Switching off cookies will still allow you to view the majority of content on our site, however, it will prevent you logging in and so accessing personalised information. It will also stop us remembering your login User ID, if you ask us to do so, and may restrict your use of our interactive tools and of some services available through linked sites.

4.4. Further information about cookies

If you would like to opt out of, or restrict the use of cookies when visiting our, or any other third party's website, you are able to adjust the settings in your Internet browser to do this. Exactly how this is done will depend on which browser you use for access to the Internet. Each browser has its own variation on how this can be achieved, but it is usually under 'Settings' which can be found at the end of the Search bar, e.g. on Chrome it is found as follows:



You then need to go to "Advanced", then "Privacy and Security", then "Content Settings" and "Cookies" and choose the most appropriate setting for yourself.

Users should check their Internet browser for details of how to amend, remove or restrict the use of cookies on their computer, tablet or other internet enabled device.

For further information about cookies, please refer to:

- Find information on internet browser cookies on the Information Commissioner's website

4.5 Third party content and linking to other websites

This privacy policy applies only to our website. We are not responsible for privacy practices within any other websites. You should always be aware of this when you leave our website and we encourage you to read the privacy statement on any other website that you visit. We embed external content from third-party websites such as YouTube, Twitter and LinkedIn including cookies. This content is not published on our website. It is delivered using devices and services from third party sites that can be inserted into our site such as media players, RSS feeds and widgets. These websites may use cookies. Their content is subject to the privacy policy of the relevant third-party provider and not ours.

5. Information sharing and disclosure

We may share your data with specified third parties for the purposes of supplying the services you have contracted us for or if required to by law or by a regulation based on a law. We will not sell, rent or disclose your information to any third parties other than those set out in this privacy policy without your prior consent.

We do not transfer your personal data outside of the UK and the European Economic Area. Or

We may transfer your personal data outside of the UK for the purposes of backing upto a cloud server hosted by Defence Services who are based St Georges Community Hub, Great Hampton Row, B19 3JG, Birmingham, United Kingdom however your personal data is kept encrypted at all times so that it cannot be read by the service provider. All personal data is still under the remit of the GDPR, regardless of our use of storage outside the UK and the EEA.

6. Retention of Data

Personal Data will always be held for the minimum amount of time required. This will depend on a number of factors, such as the terms and length of a contract or a relevant law or regulation based on law. It will be deleted a maximum of 3 years after such a period has ended under our semi-annual data clearance procedures. Personal Data that has been gathered via our website contact forms will be held for a maximum of 3 years after the initial contact, unless additional permission is obtained from the Data Subject or a contract for services is brought into force in the interim.

Electronic Personal Data is encrypted and held in a secure manner on physical and cloud-based services. The encryption used meets all current requirements for encrypted services and is updated regularly to ensure that it remains fit for purpose. Electronic data is deleted following a secure process to ensure there is no lapse in security at the point of deletion.

Paper based Personal Data is held in secure, fire-proof, locked cabinets. It is destroyed under contract with a secure data destruction company.

7. Your Rights

Under current legislation, Data Subjects have the following rights:

- **To be informed** – This policy is one of ways in which Defence Security informs you how and why we process your data
- **Of Access –** All Data Subjects have the right to quest access to all of the data we hold on them. Any Data Subject requests received will be reviewed and responded to within one calendar month of receipt of the request. Most requests will be fulfilled free of charge, however, Defence Security reserves the right to charge a reasonable administration fee for any requests deemed to be excessive, unfounded or repetitive.
- **Of rectification –** Should you find that any data we hold about you is incorrect, you can ask us to correct it and we will investigate and respond within one calendar month of receipt of the request.
- **Of Erasure –** You can ask for your Personal Data to be erased permanently. All such requests will be responded to within one calendar month of the receipt of a request. Please note that, whilst

we will always endeavour to fulfil requests, there may be some instances where this is not possible due to legal or regulatory reasons. We will always provide a full explanation in any such instances.

- **To restrict processing –** If you do not wish for your data to be erased, you may ask for it to be restricted so that we continue to hold it but not process it or use it in any way – we would essentially 'archive' your data. This is only applicable in certain circumstances, however we will look at all requests and respond within one calendar month of the receipt of a request.
- **To data portability –** All electronically held data can be transferred to another company in a structured, commonly used and machine readable format on request. Please note that this will only include the data you have provided to us and not any ancillary data produced as a result of the services we have created during the provision of our services or where that data includes information regarding a third party. All requests for moving data will be responded to within one calendar month of a request being received.
- **To Object –** You can object to our processing data for the purposes of marketing, scientific/ historical research and statistics, or legitimate interests or in the performing of a task in the public interest /exercise of official authority (including profiling). All such requests shall be responded to within one calendar month
- **Rights related to automated decision making, including profiling –** The GDPR sets out specific rights in relation to automated decision making. Please note that Defence Security does not use any form of automated decision making system whilst processing your data.
- **To complain –** You have the right to raise a complaint regarding the processing of your data or our response to a request under the above rights. As part of this, you also have the right to escalate your complaint to a supervisory authority. In respect of data handling, you have the right to escalate your complaint to the Information Commissioner's Office (ICO). Please go to https://ico.org.uk/for-the-public/raising-concerns/ for full details.

Data Subjects have the right to withdraw their consent to our processing their data at any time.

In respect of any of the rights indicated above, if you would like to make a request, require further information, or have a complaint regarding our processing of your data please contact us at: Email: basit@defence-security.co.uk

Website: www.defence-security.co.uk

Address: Defence Security
St Georges Community Hub
Great Hampton Row
Birmingham
B19 3JG

Telephone: 0121 448 1661

8. Changes to this policy

We may make changes to this privacy policy at any time. Changes will be posted on our website and are effective immediately, except where they relate directly to a contract for services where all changes will be subject to the agreements in that contract. Regularly reviewing this Policy ensures that you are always aware of what information we collect, how we use it and under what circumstances, if any, we will share it with other parties.

Quality Assurance Policy

Defence Security are committed to providing fit for purpose qualifications through our Awarding Organisation, BIIAB.

Our commitments

Defence Security is committed to ensuring that our learners are given the right opportunities and support in order for them to achieve all that they are capable of achieving.

We will support learners by:

- Providing current and up to date information in relation to the qualifications that we offer
- Identifying the correct qualification for their needs.
- Offering points of referral for any needs that we are unable to meet.
- Providing a clear and transparent fees list
- Providing any pre-course information or guidance in good time
- Ensuring delivery staff, assessors and quality assurers are occupationally competent
- Ensuring learners are aware of the assessment requirements of the qualification
- Ensuring learners have fair access to assessment
- Ensuring learners are aware of the process where competence has not been shown
- Ensuring learners are aware of our appeals and complaints procedures
- Ensuring successful learners receive certificates within good time.

Promoting our regulated qualifications

Where it has been identified that a learner will be undertaking a regulated qualification, it is important that they are not misleading into undertaking an unregulated course. We therefore consider the following when promoting our regulated qualifications:

- Titling
- Use of logos
- Access to qualification specifications
- Fees
- Logistical information

Titling

To ensure learners are not misled, all of our regulated qualifications are identified by their official title. The titles are constructed as follows:
BIIAB/ LEVEL/TYPE/SUBJECT/(FRAMEWORK), an example is:
Level 2 Award in safeguarding and protecting Children and Young People (RQF)

We avoid using similar terms for unregulated courses.

Use of logos

Logos help learners to identify any accreditations related to the qualification. Inappropriate or incorrect use may again mislead our learners. Some logos are prohibited from use, therefore we:

- Do not use regulator logos on any of our materials. Regulator logos include Ofqual, CCEA and Qualifications Wales
- Do not use any other logos protected by Crown copyright i.e. HSE
- Do not use logos of memberships or associations that are not directly linked to the qualifications
- Ensure the BIIAB logo only appears on web pages or promotional materials promoting BIIAB qualifications or on generic webpages such as "contact us" or "home"

Where logos are used, we ensure we comply with any guidance in their correct usage.

Access to qualification specifications

A qualification specification for each qualification has been created by BIIAB.
We ensure learners have access to the qualifications by emailing a copy on request.

Fees

To ensure learners are not disadvantaged by additional or hidden fees we have a transparent list of fees. This fees list ensures learners are aware of any costs associated with under taking qualifications provided by us.

Our fees list outlines costs associated with:

- Undertaking the qualification
- Cancellations
- Late payments
- Learner registration
- Assessments
- Certification
- Equipment i.e. course manual
- Appeals
- Replacement certificates

Our fees list is available on request

Logistical information

Some learners may have difficulty accessing courses in certain locations or at certain items and dates. It would be unfair to accept a learner onto a course for them to find out they are unable to attend for the required duration.

We therefore ensure prospective learners are made aware of the logistical information prior to accepting bookings.

Logistical information is available on request.

Booking confirmation and pre-course information

To ensure learners have sufficient preparation time we will ensure, once bookings have been made, we will confirm their place and reconfirm the details of the venue, dates and times and any other logistical information; i.e. parking etc

Where required by the qualification, we will ensure learners receive copies of any course materials in reasonable time.

Staff competence

We are committed to ensuring our delivery, quality assurance and office staff are competent and conversant in our products and services.

Our staff that deals with customer enquiries and bookings are often relied on by learners to ensure that the course of study they require is what they book onto.

We therefore ensure staff are aware of the needs and benefits of each qualification. They are also aware of where they can access additional information for uncommon questions and requests.

In order to continually provide suitable information to learners we record customer queries. This enables us to inform BIIAB of any queries and to update our staff with correct, current information.

We ensure that those involved in the delivery, assessment and quality assurance of qualifications are suitably qualified and experienced and meet at least the minimum requirements outlined in the BIIAB delivery manuals for each qualification.

Our centre manager is responsible for ensuring that we retain copies of CVs, certificates and activity logs for our delivery, assessment and IQA staff. These are available on request to BIIAB.

Staff responsibilities

Below is an outline of our roles and responsibilities in relation to the delivery and assessment of BIIAB qualifications.

The Centre Manager (CM) is responsible for:

- Planning and auditing course delivery and the quality assurance system
- Monitoring the Internal Quality Assurance (IQA) Strategy
- Ensuring compliance with BIIAB requirements
- Recruitment of course delivery and quality assurance team
- Writing and updating policies and procedures
- Liaising with external auditors and external quality Assurer(s) (EQA) including organising visits.
- Ensuring AO/EQA recommendations are carried out

Internal Quality Assurer is responsible for:

- The quality of assessment and the IQA of assessment
- Compiling an overall IQA Strategy
- Leading the IQA team planning process
- Monitoring and observing internal quality assurers
- Providing or organising training and guidance for internal assurers and assessors
- Reporting issues, trends and concerns to the CM
- Planning individual IQA activities
- Monitoring the assessment practise of assessors
- Verifying the accuracy, consistency and quality of assessors' decisions
- Modifying practise and procedures as a result of evaluation
- Maintaining a record of their own professional development

Trainer/Assessor is responsible for:

- Planning, managing and delivering courses
- Conducting formative and summative assessment
- Collating and preserving learner portfolios where relevant
- Agreeing an individual learning plan with learners as appropriate
- Providing all the paperwork needed to maintain the IQA process
- Providing feedback on assessment practice
- Providing guidance and support to meet the assessment requirements of courses
- Maintaining a record of their own professional development
- Reporting to Line Managers and/or Centre Manager

Assessment

Assessment is a key area for quality assurance. Failures or discrepancies in assessment show that a learner has been unsuccessful in achieving the qualification they have set out to achieve. This, in turn prompts us to look for any failings in our systems.

BIIAB has provided us with documents to support the undertaking of assessments. For some qualifications these documents include MCQ papers. Others require more input from the assessor, for example those qualifications that require a learner to build a portfolio of evidence.

Regardless of whether assessments are created by BIIAB or within Defence Security, we are responsible for ensuring that all assessments remain compliant with the principles of VCARS.

- Valid
- Current
- Authentic
- Reliable
- Sufficient

Where we have identified that assessments may not meet these principles, centre manager will be responsible for reporting our concerns to customersupport@biiab.co.uk

Contributing factors to failures in assessment

There are several reasons why a learner may not yet be competent. It is our responsibility to ensure learners have sufficient opportunities to succeed and therefore failures in assessment encourage us to consider:

- Was the qualification correct for the learners needs?
- Did the learner meet the pre-requisite(s), i.e. language, abilities?
- Was the qualification delivered at an appropriate time/location?
- Were opportunities for reasonable adjustments missed?
- Was the teaching and learning appropriate to the needs of the learner?
- Was the learner aware of the assessment criterion?
- Was the learner suitably prepared for assessment (i.e. had enough recapping and practice time)?
- Was the learner aware that they were being assessed?
- Did the assessor assess to the standardised criteria?

With this is mind it is also our responsibility to ensure learners are successful based on each of the above being in place and not because of reasons that may lead to cases of malpractice.

Undertaking the assessment

Each qualification has different assessment requirements. We will therefore ensure all assessment and quality assurance staff have suitable access to relevant BIIAB qualification delivery manuals.

Access to fair assessment

How we ensure candidates have access to fair assessment can be found in our access to fair assessment policy. This has been written to reflect the requirements of BIIAB, outlined in their reasonable adjustments policy and qualification delivery manuals.

Quality assurance of assessment

To ensure assessments are fit-for purpose, assessor and IQAs have a range of responsibilities:
The assessor should ensure that the quality of assessment is assured by;

- Planning and facilitating formative assessment throughout the course using a range of methods
- Planning and facilitating summative assessment as per Qualification Network guidelines
- Ensuring all learner papers are marked correctly
- The confidentiality and safety of assessment papers and/or leaner portfolios is maintained
- Being familiar with and following the assessment requirements as outlined by Qualifications Network
- Cooperating with the Internal Quality Assurance Team and EQA visits

The Internal Quality Assurer (IQA) should ensure that the quality of assessment is assured by;

- Verifying the suitability of lesson plans and assessment tools
- Sampling the work of trainer/assessors from each stage of the process
- Observing trainer/assessors' performance

- Sampling candidate work

Risk rating assessor/IQAs

The quality of assessment and quality assurance can be affected by the assessors and verifiers; whether this is because of inexperience or even complacency. Because of this, we assess assessment and quality assurance staff on a risk basis. The level of risk is recorded using a "traffic light" system, with green being low risk and red being high.
Each assessor's level of risk is recorded.
Examples of contributing factors to each individual's level of risk are outlined below.

High Risk

Newly appointed trainers/assessors/IQA staff
Not yet qualified trainers/assessors/IQA staff
Trainers/assessors/IQAs that have not updated their practise or with no record of CPD
Trainers/assessors/IQAs with frequent remedial actions identified via observation reports
Trainers/assessors/IQAs having made unsafe decisions
Newly appointed trainers/assessors/IQA staff
Not yet qualified trainers/assessors/IQA staff
Trainers/assessors/IQAs that have not updated their practise or with no record of CPD
Trainers/assessors/IQAs with frequent remedial actions identified via observation reports
Trainers/assessors/IQAs having made unsafe decisions

Medium Risk

Trainers/assessors/IQAs with few remedial actions identified
Qualified and experienced assessors new to the centre

Low Risk

Trainers/assessors/IQAs that demonstrate, consistently, up to date practise and have rare remedial actions identified on sampling.

Dealing with learners that are not yet competent

The integrity of a qualification and associated assessments should be called into question if there are a significantly high number of successful candidates.

Therefore, on occasion, it should be accepted that some learners will fail to achieve the desired level of competence.

Where we have ensured learners are aware of the required standard, the learner should not be surprised if the assessment decision is that they are not yet competent.

Each learner that is not yet competent will be provided with feedback on where any weaknesses appear to lie. We will then ensure suitable and sufficient support is provided in order for skills and knowledge gaps to be filled.

We will then arrange a re assessment. Learners should already be aware of any reassessment fees.

Appeals and complaints

On occasion candidates may not be satisfied with the decisions related to their assessments. They are therefore able to appeal these decisions.
The processes, including escalations are outlined in our appeals policy. This is available to candidates on request.

Processing of certificates

On successful completion of their qualification learners have the right to receive their certificate. We will ensure the swift registration of results onto the BIIAB system. We will also ensure that once received certificates are signed and distributed as soon as possible.

Where we receive replacement certificate requests, we will ensure that the identity of the candidate is confirmed and that requests are registered with BIIAB.

Quality assurance activities

To ensure the quality of our processes the centre manager is responsible for ensuring the following quality assurance activities are undertaken:

- Website audit
- Marketing materials audit
- Customer service audit
- Fees list audit
- Staff records audit
- Policy audit

These audits are undertaken on an annual basis or where a significant change occurs. Results of audits are recorded and retained for at least 3 years.

In addition to auditing our quality process we also undertake verification activities in relation to the assessment.

Planning IQA Activities (visits)

The centre manager is responsible for producing a sampling plan based on the current risk rating for each individual trainer/assessor. The sampling plan would identify who requires an IQA assessment, what units need to be verified and when.

Individual IQA staff should then produce an IQA Activity Plan for each activity they will be undertaking. This plan outlines what units/outcomes are to be verified, how the assessment will take place (methods), any resources needed by the IQA, any special needs identified by the assessor, how feedback will be given and how outcomes will be recorded. This plan ensures transparency, consistency and standardisation across the IQA team. Verification visits can be unnerving for some individuals and transparency can help to reassure trainers/assessors of what to expect on the day of the visit. As such, it is important this plan is shared with them and the Centre Manager in advance – 48 hours minimum notice is standard.

The IQA may choose which assessment methods to use from the following;

- Observation of trainer/assessor performance
- Sampling of trainer/assessor work
- Sampling of learner work
- Witness statements (from learners/co-workers)
- Learner Evaluation
- Learner Interviews
- Verification of lesson plan validity and application

Sampling Paperwork

The amount of paperwork reviewed by our IQA's is comparative to the assessor's current risk rating. For example, a high risk assessor will have all paperwork completed at the time of the visit reviewed by the IQA to ensure that marking is correct and documents have been completed properly and according to centre policy.
For a medium risk assessor it is sufficient to review only half of written papers (50% of the class) and for low risk IQAs will sample a small percentage, such as 25% of the class.

Feedback is provided to the Assessor by the IQA both verbally and written as soon as possible after the IQA visit. Feedback is also provided to IQAs by the centre manager as soon as possible after receiving their reports.

To differentiate who has marked/reviewed questions papers/assignments/reports etc is important that we have a system in place that allows a clear and consistent audit trail. Our system is as follows:

- Assessors mark/verify work in blue or black ink.
- IQAs verify work using red ink
- Lead IQA should use a different colour to clearly show when/where they have reviewed IQA reports or have some way of distinguishing themselves from the other IQAs
- EQAs verify using green ink

Conducting an IQA Activity

Our sampling activities are carried out by visiting the assessor while they are assessing, however, on some occasions it may be possible to conduct a 'remote' visit whereby data is sent to the IQA. Whichever method is used, the following steps/procedures will apply.

Planning/Preparation

IQA will produce an assessment plan detailing which assessment will be verified during the activity and what methods will be used. This plan will be shared with the assessor and the IQA.

When planning the visit, the IQA will ensure they have the correct contact details and site details and have planned their journey to arrive at the agreed time. For some qualifications sampling activities may include a review of the formal teaching session to verify if learning outcomes have been met and formative assessment conducted as well as the summative tasks.

This is not a review of teaching practice or subject knowledge, simply verification that the outcomes are being covered. It would be difficult for assessment criteria to be met by a learner if they had not received the correct training prior to assessment. A record of this observation should be kept.

Arriving on site

Upon arrival the IQA should inform the assessor of their arrival but without causing unnecessary disturbance or interruption to any learning sessions. When convenient the IQA will review the assessment plan with the assessor and both parties should initial their agreement on the plan.

The IQA may at this point ask to see the course register to verify it has been completed properly and to also have ready the learner information they will need to complete their reports.

During the sampling activity, especially during observation of training / assessment, the IQA should ensure they place themselves in a suitable position whereby they can monitor activity but not cause a disturbance to the learners or be located in such a way that they would cause unnecessary anxiety for a candidate undertaking assessment.

Collecting Evidence

During the sampling activity the IQA may observe the delivery of subject content and formative assessment and record how each learning outcome for the unit is covered using the 'IQA' observation form.

During the summative assessment the IQA will observe learners demonstrating skills or completing test papers and will make notes of how assessments were conducted including the outcomes.

Observations / feedback will be referenced against the assessment guidelines outlined in the BIIAB qualification delivery manuals. Paperwork completed by candidate and assessors will be reviewed and the IQA will initial, ideally in red ink, to show the work has been reviewed.

The IQA will record the evidence collected on the 'IQA Sampling Plan' form. Feedback and development points identified are recording on the 'IQA Report Form'.

IQA Evidence Collection – Tool Box

In addition to the standard forms described above, our IQA's have a 'tool box' of resources which can be used to substantiate the outcome of their report. For example, if our IQA has not been able

to directly witness or evidence an outcome being met, it may be appropriate to interview a learner(s) or to ask further questions of an assessor. This can be particularly useful if there are discrepancies in observed practice and feedback from the assessor or learners.

Learner Evaluation Forms

Learner evaluation forms can be used when a sampling activity is taking place after an assessment has been conducted. This may have been necessary due to IQA / Assessor availability or due to delays in arrival or a change to the expect course delivery / assessment schedule. They can be used at other times but are best suited for these occasions

Learner Interviews

Learner interviews can be used to support observed practise using the 'Learner Interview Checklist' or for longer interviews where assessment has not been observed using the 'Learner Interview Sheet'. When conducting interviews, IQAs ensure the activity does not cause unnecessary disruption to the class and does not detain a learner from participating in course delivery.

Assessor Question Sheet

This can be used to evaluate underpinning knowledge of an assessor on the assessment criteria such as reasonable adjustment and marking schedules.

Completing the Activity

Assessor Feedback

At the end of the sampling activity the IQA will provide the assessor with an opportunity to reflect on their performance and to identify any development points or concerns. The IQA will need to liaise with the assessor on the best time and place to conduct the feedback / review session but, whenever possible, this should be completed at the time of the visit. On rare occasions, the assessor may be requested to submit a written reflection; however, this must be clearly detailed in the IQA report and action plan. Feedback should relate to the learning outcomes and assessment criteria only.

Reports

Upon completion of the verification activity, the IQA will submit their reports to the centre manager as soon as possible. Reports should be sent electronically.

Should any urgent issues have been identified during the activity, the IQA will report to the centre manager immediately.

Standardisation

Standardisation ensures the validity and reliability of the IQA process. IQA team members are required to attend regular meetings to review best practise, raise ideas / concerns and to receive updates on process / policy / training etc.

Standardisation events are also organised by BIIAB. Attendance of these meetings/events contributes to individual Continuous Professional Development (CPD) portfolios. CPD is an important part of the quality assurance process and IQAs maintain a record of their CPD activities.

A key component of a CPD record is reflective statements.

Policy review date: April 2023

Reasonable Adjustment Policy

Defence Security and BIIAB believe that a learner's individual characteristics and work situation must be taken into account in order to provide the appropriate access to training and assessment.

Defence Security will endeavour to review individual needs with learners upon registration/attendance. Where a learner has been identified as requiring additional support Defence Security will agree an Individual Learning Plan and will provide appropriate advice, guidance and support to those Learners identified as having special assessment needs.

Where required we Defence Security will make reasonable adjustments to assessment which may include (but not be limited to);

- Allowing additional time to complete written tests/tasks
- Offering the use of a scribe for written tests
- Accepting verbal responses to written questions (these must be recorded)
- Allowing the use of transcribed materials to prepare/support a learner for assessment
- Use of visual aids (e.g. videos) to support formal questions (e.g. to identify different medical conditions)
- Allowing the use of a translator (including sign language) to prepare/support a learner through assessment.
- Changing the layout or venue of the assessment area to allow access

Any adjustments made will ensure that the assessment criteria are still met and that BIIAB standards are upheld.

Where the Centre is unable to agree to reasonable adjustments we will contact BIIAB for further advice and guidance.

Abdul Basit — April 2022

Signed on behalf of Defence Security — Date

April 2024

Policy review date

Third Party Vendor Policy

The purpose of this policy is to establish rules and operating parameters for third party vendors' access to company information, their operator responsibilities, and protection of Defence Security assets, data, and Personally Identifiable Information (PII). Third party vendors may collect, store and maintain confidential information and PII. Setting appropriate limits and control on third party vendors helps reduce the risk of security incidents, financial liability, loss of community and embarrassment.

This policy applies to all Defence Security staff responsible for negotiating or executing third party contracts.

Due Diligence

Prior to entering into any agreement or contract, Defence Security staff shall follow due diligence in selecting third party vendors. Third parties must comply with all applicable state procurement, Defence Security policies, practice standards, and agreements.

Vendor Responsibilities

The following general responsibilities shall be provided by vendors entering contracts with Defence Security:

- Third party vendors shall provide Defence Security a point of contact for contract terms and service offering implementation. A Defence Security point of contact will work with the third-party vendors to ensure the vendor is in compliance with this policy.
- Defence Security shall maintain a list of all subcontracted providers and the services performed by each. Defence Security may request on-demand and maintain copies of all agreements with service providers as appropriate.

Third party contract terms and provisions

All contract terms and agreements with third party service providers shall specify the following terms and conditions:

- Data and personnel confidentiality terms shall protect all Defence Security Confidential Information and PII.
- Role-based controlled user access to Defence Security resources and access shall be limited to only those systems to which the vendor provides services.
- Vendor data privacy and information security procedures and protocols shall be made available and meet Defence Security requirements for the return, destruction, or disposal of information in the service provider's possession at the end of the agreement.
- The service provider shall only use Defence Security's information and systems for the purpose of the direct business agreement. No other uses are allowed unless expressly granted in writing by Defence Security.

- Any information acquired by the service provider through the course of operational contract execution shall not be used for the service provider's own purposes or divulged to others without the express written consent of Defence Security.
- Defence Security will be provided with a full list of all staff working on the contracted services. The list shall be updated and provided to Defence Security within twenty-four hours of staff changes.
- On-site service provider staff members must adhere to all internal facility security protocols and procedures. Upon completion of contracted work, service providers shall return all security access cards and identification.
- Service provider staff members with access to Defence Security confidential or learner PII must be cleared to handle that information. Third party access to PII and confidential data shall be activated only when needed and enabled only to the level and degree indicated by the contract statement of work.
- System access shall be deactivated/disabled after services have been completed. IDs used by vendors to access, support, or maintain system components via remote access shall only be enabled during the time period needed and disabled when not in use.
- Third party service provider access to systems and software shall be monitored during use as required by the sensitivity and confidentiality of the information.
- Service providers with remote access to Defence Security systems shall use all prescribed tools and procedures to access systems remotely.
- Service provider personnel shall report all security incidents directly to the project supervisor, head of centre and accountable person. Security incident management responsibilities and details must be specified in the contract agreement and specific to data incident/breach notification, procedures, notifications and remedies.
- The service provider shall follow all applicable Defence Security change control processes and procedures when working on Defence Security systems.
- Regular work hours and duties shall be defined in the agreement. Work outside of defined parameters must be approved in writing by appropriate Defence Security management.
- Service provider access shall be uniquely identifiable and password/access management must comply with all Defence Security requirements
- Upon termination of the service provider or at the request of Defence Security, the service provider will return or destroy all information and provide written certification of that return or destruction within twenty four hours.
- Upon termination of contract or at the request of Defence Security, the service provider must surrender all identification badges, access cards, equipment, and supplies immediately. Equipment and/or supplies to be retained by the service provider must be documented by management.

- Service providers are required to comply with all Defence Security auditing requirements, including the auditing of the service provider's work.
- Service providers shall include explicit coverage of all relevant security requirements. This includes controls over the processing, accessing, communicating, hosting or managing the organisation's data or adding or terminating services or products to existing information.
- Service providers shall include explanations of security mechanisms (e.g., encryption, access controls, and security leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration, or destruction.
- Service provider contracts shall require the provider to acknowledge responsibility for securing Defence Security sensitive information the provider possesses or otherwise stores, processes, or transmits on behalf of Defence Security
- Agreements with third party service providers shall specify that the third party service provider will notify Defence Security within one day of discovery of a service provider security incident/breach. Upon such notification, Defence Security shall have the right to terminate the agreement with the service provider. Provisions within the contract shall ensure that the service provider pay for all costs incurred to remedy the breach including, if appropriate, notifying customers, and any related expenses or damages levied due to the incident and related disclosure.

Other provisions

When dealing with PII, service providers shall provide an on-line and print description of security and privacy directives, guidelines, policies, and security safeguards that protect the learners PII.

No contracts shall be entered into by Defence Security where the standard vendor contract template is not used and all applicable terms applied. Any negotiations between vendor and Defence Security must be completed through Defence Security.

Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy. Operational compliance can be demonstrated through:

- On-demand review of standard agency contracts with third party providers.
- Review of departmental operational procedures for compliance.
- Random review of current contracts for terms compliance.

This policy is to be distributed to all Defence Security staff and management responsible for negotiating and managing vendor contracts within Defence Security. Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

Policy review date: April 2024