



The United Kingdom Event Industry Academy

In association with

The Asia Pacific Institute for Events Management Academy



POLICIES & PROCEDURES 2024 – 2025

1. Data Protection Act 2018 Policy

Introduction

This Policy sets out the obligations of UKEIA & APIEM, (“the Company”) regarding data protection and the rights of customers and business contacts (“data subjects”) in respect of their personal data under Data Protection Act 2018 (Formally EU Regulation 2016/679 General Data Protection Regulation (“GDPR”).

The Data Protection Act 2018 defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets the Company’s obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

The Data Protection Principles

This Policy aims to ensure compliance with the Data Protection Act 2018. The Data Protection Act 2018 sets out the following principles with which any party handling personal data must comply. All personal data must be:

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and

organisational measures required by the Data Protection Act 2018 in order to safeguard the rights and freedoms of the data subject.

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

The Rights of Data Subjects

- The Data Protection Act 2018 sets out the following rights applicable to data subjects
- The right to be informed'
- The right of access,
- The right to rectification,
- The right to erasure (also known as the 'right to be forgotten'),
- The right to restrict processing,
- The right to data portability,
- The right to object; and
- Rights with respect to automated decision-making and profiling.

Lawful, Fair, and Transparent Data Processing

The Data Protection Act 2018 seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Data Protection Act 2018 states that processing of personal data shall be lawful if at least one of the following applies:

- The data subject has given consent to the processing of their personal data for one or more specific purposes;
- The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
- If the personal data in question is "special category data" (also known as "sensitive personal data") (for example, data concerning the data subject's health), at least one of the following conditions must be met:
- The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

- The processing relates to personal data which is clearly made public by the data subject;
- The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

Specified, Explicit, and Legitimate Purposes

The Company collects and processes the personal data set out in this Policy. This includes:

- Personal data collected directly from data subjects **OR**
- Personal data obtained from third parties.
- The Company only collects, processes, and holds personal data for the specific purposes set out in this Policy (or for other purposes expressly permitted by the Data Protection Act 2018).
- Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data.

Adequate, Relevant, and Limited Data Processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

Accuracy of Data and Keeping Data Up-to-Date

- The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject.
- The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

Data Retention

- The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
- When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
- For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction,

or damage. Further details of the technical and organisational measures which shall be taken are provided later in this Policy.

Accountability and Record-Keeping

The Company's Data Protection Officer is David Hind,
E-Mail: davidwghind@gmail.com
Tel: 0113 2400862

The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the Data Protection Act 2018 and other applicable data protection legislation.

- The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:
- The name and details of the Company, its Data Protection Officer, and any applicable third-party data processors;
- The purposes for which the Company collects, holds, and processes personal data;
- Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by the Company; and
- Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

Data Protection Impact Assessments

- The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data.
- Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:
 1. The type(s) of personal data that will be collected, held, and processed;
 2. The purpose(s) for which personal data is to be used;
 3. The Company's objectives;
 4. How personal data is to be used;
 5. The parties (internal and/or external) who are to be consulted;
 6. The necessity and proportionality of the data processing with respect to the
 7. purpose(s) for which it is being processed;
 8. Risks posed to data subjects;
 9. Risks posed both within and to the Company; and
 10. Proposed measures to minimize and handle identified risks.

Keeping Data Subjects Informed

The Company shall provide the information set out in section (i) below to every data subject:

Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

- a) if the personal data is used to communicate with the data subject, when the first communication is made; or
- b) if the personal data is to be transferred to another party, before that transfer is made; or
- c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

(i) The following information shall be provided:

- Details of the Company including, but not limited to, the identity of its Data Protection Officer;
- The purpose(s) for which the personal data is being collected and will be processed (as detailed in this Policy) and the legal basis justifying that collection and processing;
- Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- Where the personal data is to be transferred to one or more third parties, details of those parties;
- Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the “EEA”), details of that transfer, including but not limited to the safeguards in place,
 - Details of data retention;
 - Details of the data subject’s rights under the Data Protection Act 2018;
 - Details of the data subject’s right to withdraw their consent to the Company’s processing of their personal data at any time;
 - Details of the data subject’s right to complain to the Information Commissioner’s Office (the “supervisory authority” under the Data Protection Act 2018);
 - Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
 - Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

Data Subject Access

- Data subjects may make subject access requests (“SARs”) at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.
- Data subjects wishing to make a SAR may do so in writing, using the Company’s Subject Access Request Form, or other written communication. SARs should be addressed to the Company’s Data Protection Officer at UKEIA & APIEM, 8, Oakwood Grange Lane, Leeds, LS8 2PF Tel: 0113 2400862 Email: davidwghind@gmail.com

- Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
- All SARs received shall be handled by the Company's Data Protection Officer.
- The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Rectification of Personal Data

- Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.
- The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
- In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

Erasure of Personal Data

Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

- a) It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
- b) The data subject wishes to withdraw their consent to the Company holding and processing their personal data;
- c) The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so),
- d) The personal data has been processed unlawfully;
- e) The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed. In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

Restriction of Personal Data Processing

Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

Objections to Personal Data Processing

Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling) and processing for scientific and/or historical research and statistics purposes.

Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Data Protection Act 2018, "demonstrate grounds relating to his or her particular situation". The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by the Company:

Electronic and hard copy Learner records

Data Security - Transferring Personal Data and Communications

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- All emails containing personal data must be encrypted using Encryption software;
- All emails containing personal data must be marked "confidential";
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted using deletion software;
- Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail Registered or 1st or 2nd Class Signed For post; and
- All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”.

Data Security – Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

- All electronic copies of personal data should be stored securely using passwords and data encryption;
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
- All personal data stored electronically should be backed up at least daily with backups stored onsite. All backups should be encrypted using data encryption’
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of the Data Protection Officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and
- No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Data Protection Act 2018 (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

Data Security – Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

Data Security - Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

- No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that

they do not already have access to, such access should be formally requested from The Data Protection Officer,

- No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of The Data Protection Officer,
- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and
- Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of David Hind to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

Data Security - IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security:

- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols;
- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates after the updates are made available by the publisher or manufacturer, unless there are valid technical reasons not to do so; and
- No software may be installed on any Company-owned computer or device without the prior approval of the Company.

Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Data Protection Act 2018 and under this Policy, and shall be provided with a copy of this Policy;
- Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;
- The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Data Protection Act 2018 and this Policy by contract;
- All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Data Protection Act 2018; and
- Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Transferring Personal Data to a Country Outside the EEA

The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Data Protection Act 2018); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
- The transfer is made with the informed consent of the relevant data subject(s);

- The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);
- The transfer is necessary for important public interest reasons;
- The transfer is necessary for the conduct of legal claims;
- The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
- The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

Data Breach Notification

- All personal data breaches must be reported immediately to the Company's Data Protection Officer.
- If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
- In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
- Data breach notifications shall include the following information:
 - The categories and approximate number of data subjects concerned;
 - The categories and approximate number of personal data records concerned;
 - The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
 - The likely consequences of the breach;
 - Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

This policy has been approved & authorised by:

Name:

Professor David Hind

Position:

Chief Executive, UKEIA

Date:

1st January 2024

Signature:

David W. S. Hind

Review of Policy:

31st December 2024

2 – Equal Opportunities Learner`s Charter

“Everyone has a part to play in ensuring we achieve equality of opportunity. UKEIA & APIEM believe that a positive attitude towards equality and diversity is right for our people, our clients and our business suppliers. This means that we must encourage all our people to welcome diversity and respect each person’s individuality”.

UKEIA & APIEM is committed to ensuring that the admissions process will be open and transparent, and that no individual or group receives less favourable treatment by virtue of age, disability, economic status, faith, gender, marital status, sexuality, race, colour, and nationality, ethnic or national origin.

The following Learner Charter has been drawn up stating the standards of service you can expect to receive as a learner of UKEIA & APIEM:

Using UKEIA & APIEM you can expect...

- to receive a highly quality learning experience
- to be given equal opportunities and treated fairly
- to be treated with courtesy
- to have access to advice, guidance and support to ensure your choices are informed ones and that your learning needs are met
- to learn in a healthy and safe environment
- to be provided with timely and appropriate information on your progress
- to have staff listen to any issues, suggestions or concerns you may have, and to respond in a relevant manner

In turn UKEIA & APIEM would like you to:

- be fully committed to your course
- treat our staff with courtesy
- provide us with appropriate information to help us meet your learning and assessment needs
- ensure that your behaviour contributes to a healthy and safe environment
- abide by any rules specifically relating to online assessment
- communicate issues, suggestions or concerns using the procedures outlined in your Student Handbook.

If for any reason you wish to make a formal complaint, then please access our formal complaints procedure on the website or email contact@theapiem.com. This policy has been approved & authorised by:

Name:

Professor David Hind

Position:

Chief Executive, UKEIA

Date:

1st January 2024

Signature:

David W. G. Kind

Review date of the policy:

31st December 2024

3 – Appeals Procedure

The UKEIA & APIEM provide a formal route for our scholars wishing to appeal against an assessment decision. All scholars are assessed against the relevant learning outcomes for the course and UKEIA assessment criteria, where applicable. Assessment decisions are made by internal Assessors.

Areas for Appeal

The UKEIA & APIEM Appeals Policy enables scholars in certain situations to make a formal appeal against a recommendation or assessment decision relating to:

1. the Assessor's decision on any element of assessment that differs to that of our Internal Quality Assurer's decision (for example, if an internal assessment has been marked by the Assessor as achieved but the Internal Quality Assurer disagrees with this decision).
2. an application for a reasonable adjustment or special consideration submitted to UKEIA & APIEM for approval.
3. The UKEIA & APIEM final, overall assessment decision for a CPD Course.

Grounds for Appeal

The following is a list of examples and is not exhaustive:

- A reasonable adjustment was refused without reason, or a decision to limit a request for a reasonable adjustment proved to be inappropriate or insufficient.
- The scholar requested special consideration, but this does not seem to have been applied.
- There was inappropriate or irregular conduct on the part of the Assessor.

Appeals Process

Stage 1

The scholar should discuss on the day they receive the assessment decision their intention to appeal that decision directly with the Assessor responsible for informing the scholar of that decision. If the scholar is dissatisfied with the outcome of this discussion, the scholar should request a 'Scholars Appeals Application' form which can be emailed to you. The scholar must

submit this form within five days of the date of the assessment and include with it any supporting evidence (see additional notes below). Appeals received after this time will not be heard.

Stage 2

Once received by UKEIA & APIEM, our designated Internal Quality Assurer (“IQA”) will investigate the appeal and respond in writing to the scholar with a decision within 20 working days of receipt of the form. If the scholar is dissatisfied with the IQA’s decision, the scholar should make a complaint directly to the Owner of UKEIA.

Additional Notes

1. It is extremely difficult to investigate appeals without impartial evidence. Therefore, appeals against referrals in practical teaching based solely on the scholar’s disagreement with the Assessor’s decision will only be considered when accompanied by a video recording of the learner’s practical assessment.
2. The scholar has the right to video any aspect of their practical assessment using their own video recording equipment provided it does not interfere with the assessment process, other scholars, or the Assessor’s ability to carry out their role(s).
3. It is the responsibility of the scholar to arrange a video operator.
4. Prior to the assessment date and so that a decision can be made for deferral, it is the responsibility of the scholar to notify UKEIA & APIEM of any medical problem which may affect the scholar’s performance adversely in the assessment process.

This policy has been approved & authorised by:

Name:

Professor David Hind

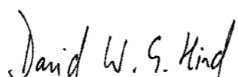
Position:

Chief Executive, UKEIA

Date:

1st January 2024

Signature:



Review date of Policy:

31st December 2024

4 – Complaints Policy & Procedures

Complaint – a grievance, problem, difficulty or concern

POLICY STATEMENT

UKEIA & APIEM recognises the importance of learner complaints and welcomes complaints as a valuable form of feedback about its services. We are committed to using the information we receive to help drive forward improvements.

This procedure outlines the aims of UKEIA & APIEM in dealing with complaints and sets out what learners can expect when making a complaint regarding a service provided by UKEIA & APIEM.

A complaint is a way of letting us know that you are not happy with a particular service. We welcome your feedback. A complaint may be about delay, lack of response, discourtesy, failure to consult or about the standard of service you have received.

So please let us know if:

- you think we have done something wrong
- we have not done something that we said we would do
- you are not satisfied with a particular service or set of services that we provide

ANONYMOUS COMPLAINTS

We understand that it might be difficult for you to complain because you are worried that your complaint could result in a poorer service. Please be assured that we treat all complaints in the strictest confidence, and that it is your right to complain. If you do not provide us with a contact name or address, it will not be possible for us to get back to you with the outcome of the investigation

PROCEDURE

In the first instance, the complaint should be discussed with the team member concerned and resolution sought within 48 hours of the incident occurring. If this is successful and a resolution is reached, the complaint should be documented on the attached Appendix (4a) and sent to the UKEIA & APIEM Administrator for filing. This should be received by the UKEIA & APIEM Administrator by the end of the next working day. There will be no further action taken.

In the case of a learner wishing to make the complaint, who feels unable to discuss the complaint with the team member concerned, the matter should be referred to the UKEIA & APIEM Course Leader within 48 hours of the incident occurring. The Course Leader should then contact the UKEIA Company Owner within the next 7 days to make them aware of the complaint. The nature of the complaint will be documented as per Appendix (4b) and sent to the UKEIA & APIEM Vice President for Academic Affairs.

On receipt of the complaint, the nature of the complaint will be brought to the attention of the team member concerned and discussed within 48 hours of receiving the complaint. The UKEIA & APIEM Vice President for Academic Affairs will then contact the learner making the complaint with a view to resolve.

If resolution cannot be found, the UKEIA & APIEM Vice President for Academic Affairs will arrange a meeting with all relevant parties and agree a resolution. This will take place within 30 days. This will be final.

The UKEIA & APIEM Administrator will maintain a record of all complaints and make these available on request. All complaints must be regarded as confidential and discussed only with those parties involved.

In the instance where the complaint is around an assessment / verification decision, then the stages outlined in the Appeals Procedure must be followed.

Appendix 4a

Record of Complaint

Name of Individual making the complaint: Location:

Date:

Nature of complaint

| |
|--|
| |
|--|

Resolution Agreed:

Signed Complainant:

Date:

Signed by UKEIA & APIEM Vice President for Academic Affairs

Date:

Appendix 4b

Referral of Complaint

Date of referral:.....

UKEIA & APIEM Vice President for Academic Affairs Name:

.....

Nature of complaint:

Date Referred to Head of Assessment Centre:.....

Actions agreed:

Signed off by the UKEIA & APIEM Vice President for Academic Affairs Date:

Signed

Complainant:.....Date

Name:

5

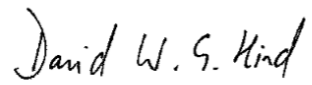
Professor David Hind

Position:

Chief Executive, UKEIA

Date: 1st January 2024

Signature:

A handwritten signature in black ink that reads "David W. G. Hind". The signature is written in a cursive style with a large initial 'D'.

Review of Policy:

31st December 2024

5 - Reasonable Adjustments Policy

Aims and Objectives of the Policy

UKEIA & APIEM have a duty under the Equality Act 2010 to make any reasonable adjustments that can be made for our learners to ensure they are not discriminated against.

We aim to facilitate open and fair access to our training for learners who are eligible for reasonable adjustments and/or special considerations without compromising the assessment of skills, knowledge, understanding or competence being measured, UKEIA & APIEM achieve this through;

Reasonable Adjustments

UKEIA & APIEM will consider requests for Reasonable Adjustments and Special Considerations. This is agreed at point of booking/registration. The learner must request within a reasonable timeframe any adjustments that may be needed to reduce the effect of a disability or difficulty, which places the learner at a substantial disadvantage. Any requests for reasonable adjustments must not affect the quality and reliability of the learning outcomes nor must they give the learner an advantage over other learners undertaking the same or similar training. Reasonable Adjustments may not be applied to training that will provide a “licence to practice” or where the learner needs to demonstrate a practical competence.

Special Considerations

A special consideration request can be made during or after a training event to reflect temporary illness, injury or indisposition that occurred at the time of the event. Any special considerations granted cannot remove the difficulty the learner faced at the time of the event and can only be a relatively small adjustment to ensure that the integrity of the training is not compromised. Special consideration may not be applied to training that will provide a “licence to practice” or where the learner needs to demonstrate a practical competence.

UKEIA & APIEM will only consider requests for Reasonable Adjustments and Special Considerations submitted within a timely manner and have completed the appropriate paperwork for these requests.

Reasonable Adjustments

A reasonable adjustment helps to reduce the effect of a disability or a difficulty that places the learner at a substantial disadvantage.

Reasonable adjustments must not affect the quality and reliability of the learning outcomes, but may include;

- Ensuring any online learning is more accessible (such as the ability to adjust display settings and provide advice/guidance on speech technology)
- assisting with an assessment of learning
- Adapting materials or providing them on coloured paper

- Re-organising the physical assessment/learning environment
- Use of mechanical and electronic aids
- Use of assistive software
- Use of low-vision aids
- British Sign Language

Reasonable adjustments must be approved and set in place before any assessment or learning is carried out.

Any assessment of work following a reasonable adjustment that has been made must be carried out in the same way as other learners.

Reasonable adjustments must never give a learner an advantage to other learners and must never affect the quality or reliability of the learning.

It is important to note that not all requests for reasonable adjustments may be granted if they are not deemed reasonable, permissible, or practical in certain situations. The learner may not need, nor be allowed, the same adjustments for all learning.

Requests for reasonable adjustments are approved by UKEIA & APIEM before any bookings/registrations are taken. They are intended to allow access to training/assessment but can only be approved if the adjustment does not;

- affect the quality and reliability of the learning
- provide an unfair advantage to other learners
- Influence or compromise the final outcome of the assessment of learning

Any requests for reasonable adjustments must be made to UKEIA & APIEM within 7 days of registration/booking or at least 28 working days before an assessment/classroom event using the appropriate paperwork. If you are unsure if a learner requires a reasonable adjustment, please speak with UKEIA & APIEM who will provide the relevant guidance.

Special Considerations

Special consideration is consideration given to a learner who was prepared and present at an assessment but may have been disadvantaged by temporary illness, injury or adverse circumstances outside of their control.

It is important to note that special consideration may not be possible where assessment requires the demonstration of practical competence, or the training provides a “licence to practice”.

Where an assessment of learning is carried out and marked by a computer, the learner will have the ability to take it later however this must be completed before any practical assessments or other learning is carried out.

A special consideration cannot give a learner an unfair advantage over other learners and must not mislead the learners’ achievement. The learner’s results must reflect their true achievement and not potential ability. UKEIA & APIEM’s decision on requests for special considerations will vary from learner to learner and one subject to another. The factors may include the severity of the

consideration, the date of assessment and the nature of the assessment such as practical or oral presentation.

The learner may be eligible for special considerations if:

- the performance in an assessment is affected by circumstances out of their control, such as recent personal illness, accident or bereavement
- alternative arrangements which were agreed in advance proved to be inappropriate or inadequate
- part of an assessment/event was missed due to circumstances beyond the control of the learner

The learner will not be eligible for special consideration if:

- the learner has not been affected at the time of an assessment by a particular condition
- part of an assessment/event is missed due to personal arrangements including holidays or unauthorised absence
- the event/assessment is affected by difficulties such as disturbances through building work, lack of proper facilities, changes in or shortages of staff or industrial disputes

Examples of circumstances where special consideration may be given are:

- terminal illness of the learner
- recent bereavement of a member of the immediate family
- serious or disruptive domestic crises leading to acute anxiety about the family
- incapacitating illness or injury of the learner
- severe car accident
- outbreak of infection where learners are in isolation
- lost or damaged work beyond the control of the learner

Special consideration will not be granted for minor illness or a minor disturbance.

Requests for special considerations are approved by UKEIA & APIEM. Applications for special considerations must be made on case-by-case basis and thus separate applications must be made for each learner. Any requests for special considerations will only be approved if they do not:

- affect the quality and reliability of the learning
- provide an unfair advantage to other learners
- influence or compromise the final outcome of the assessment of learning

Any requests for special considerations must be made to UKEIA & APIEM within 7 days of the event or assessment using the appropriate paperwork. If you are unsure if a learner requires a special consideration please speak with UKEIA & APIEM who will provide the relevant guidance.

It is important to note that special consideration will not be granted if / where learner achievement has been acknowledged and certified.

This policy has been approved & authorised by:

Name:

Professor David Hind

Position:

Chief Executive, UKEIA

Date:

1st January 2024

Signature:

David W. G. Hind

Review date:

31st December 2024

6 - Course Content and Review Policy

UKEIA & APIEM take the standard of their courses very seriously. For this reason, the below policy sets out how we ensure the standards of our service is maintained.

Course reviews are an integral part of UKEIA & APIEM`s quality assurance process.

The focus of course reviews is on:

- the appropriateness of the content and assessment method to achieve the learning outcomes,
- the course content is up to date and accurate.

Responsibility

Responsibility for course review and recommendations being addressed rests with the UKEIA & APIEM Vice President for Academic Affairs. The responsibility for the Review process lies with the company Directors.

Frequency

Each course is reviewed on an annual basis. The courses are reviewed by a Subject Matter Specialist to ensure their accuracy.

Timing

At the review date, each subject area specialist will have a 30-day period to complete the review of the given subject and all findings reported back to the UKEIA & APIEM Vice President for Academic Affairs.

The UKEIA & APIEM Vice President for Academic Affairs will then action any appropriate changes to course materials with an additional 30-day period.

Reporting

Following learning materials review, a detailed report will be provided to the UKEIA & APIEM Vice President for Academic Affairs, outlining all elements that require addressing and updating.

Name:

Professor David Hind

Position:

Chief Executive, UKEIA

Date: 1st January 2024

Signature:

David W. G. Kind

Review of Policy:

31st December 2024

7 - Responsible Marketing Policy & Procedure

Introduction

The main aim of the policy is to provide clear guidance on how UKEIA & APIEM markets itself responsibly. We are committed to delivering high-quality teaching and learning, along with exceptional customer service for our stakeholders. This extends to ensuring our services are marketed in a way that is fair, transparent, within legal guidelines and reflective of the communities we serve.

We also require that our partners and stakeholders adhere to these standards and that unsubstantiated claims aren't made. Any use of data must be verified, and sources confirmed to ensure potential customers are made aware of its origin.

We are committed to responsibly marketing our products and services and so we will regularly review our marketing communications to ensure they are aligned with these principles and that they also fit with industry best practices.

Scope

These guidelines apply to all marketing communications generated by or on behalf of UKEIA & APIEM. Within this, 'marketing' means product and services advertising and promotion in all media including, but not limited to, packaging, brand promotions, brand advertising, brand PR, product placement, sponsorship and brand experiential marketing, point of sale material, digital, online and mobile marketing plus social media.

Core Principles

We commit that our marketing communications will be honest, transparent, truthful, within legal guidelines and respectful.

Above this we also commit to:

- never mislead our customers.

- always be fair and transparent when promoting our services, enabling our customers to make informed choices. Offering impartial advice and guidance in line with our duty of care as a CPD Approved Provider.
- be legal, ethical, truthful and conform to accepted principles of fair competition and good business practice.
- comply with all UK legislative and regulatory requirements.
- avoid promoting themes associated with aggression, anti-social behaviour or violence.
- avoid any derogatory, defamatory, or offensive statements or imagery in particular about race, gender, sexual orientation, religion and political views.
- seek to prevent any unsolicited marketing that uses the UKEIA & APIEM brand without authorisation
- never knowingly advertise in media or on websites that contain extremist views or explicit content.
- never advertise in a way that could cause mental, physical or moral harm to a child.

Compliance

All new marketing colleagues and key agency personnel are aware of our Core Principles, and we review the principles regularly. In addition, refresher training is available when needed.

Our marketing team/3rd party agency members, supported by our legal, technical and communications operatives, are responsible for ensuring the compliance of all our marketing collateral.

Other, non-marketing collateral which has a customer audience (for example recruitment material or UKEIA & APIEM Newsletter communications) should also comply with these principles. Internally, all imagery is to be approved in isolation, in colour, at full/oversize and in situ/as it will be seen by the customer.

This policy has been approved & authorised by:

Name:

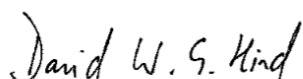
Professor David Hind

Position:

Chief Executive , UKEIA

Date: 1st January 2024

Signature:



Review of Policy will be carried out:

31st December 2024

8 - Reflective Practice Record

| | |
|-----------------------------------|-----------------------|
| Name: | Workplace: |
| Date of Activity: | Location of Activity: |
| Description of Activity or Event: | |

Reflection: What have you learnt?

Reflection: How will you use it at work? How can you pass this knowledge on to others?

Reflection: Do you need to continue your learning? Do you feel/think any differently as a result?

Signature _____

Date

9 - UAEIA & APIEM Learner Evaluation Form

Questions

What is your overall assessment of the course/event, where (1) = insufficient, and (5) = excellent

1 2 3 4 5

Which topics or aspects of the course/event did you find most interesting or useful?

Did the course/event achieve the programme objectives?

Yes No

If no, why?

Knowledge and information gained from participation at this course/event?

Met your expectations Yes No Somehow

Will be useful/applicable in my work **Definitely** **Mostly** **Somehow** **Not**
at all

How do you think the course/event could have been made more effective?

Please comment on the organization of the event (from 1 = insufficient to 5= excellent)

1 2 3 4 5

Comments and suggestions (including activities or initiatives you think would be useful, for the future)

Further comments or suggestions

THANK YOU