Data Protection and Information Security Addendum effective from 1 May 2026 (the "Addendum"). This Addendum is incorporated into the QA General Terms of Sale available at *https://www.qa.com/legal-privacy/* (the "General Terms").

1. DEFINED TERMS

1.1. For the purposes of this Addendum:

1.1.1. definitions in the General Terms shall apply; and

1.1.2. the terms "controller", "processor", "data subject", "personal data", "processing" (and any derivatives thereof) and "appropriate technical and organisational measures" have the meanings given in Data Protection Legislation and the following terms shall have the following meanings:

Agreed Purpose: means the provision or receipt (as applicable) of goods and/or services under a Contract;

Business Contact Details: means personal data confined to the following categories of information relevant to the following categories of data subject: (a) business names; (b) basic personal details; and (c) contact details, in each case of the parties' personnel used to administer the Contract;

Data Discloser: means either party when it discloses personal data to the other party in connection with the Contract;

Data Privacy Framework ('DPF'): means the EU–U.S. Data Privacy Framework, together with its UK Extension and the Swiss–U.S. Data Privacy Framework, allowing personal data to be transferred to certified U.S. organisations in compliance with applicable Data Protection Legislation;

DPF Principles: means the Data Privacy Principles issued by the U.S. Department of Commerce;

Data Protection Legislation: means all applicable data protection, privacy and electronic communications laws in the United Kingdom, the European Union and the United States, and any national implementing laws regulations and secondary legislation made under them each as amended or re-enacted and in force from time to time, including but not limited to: (i) the UK Data Protection Legislation; (ii) the General Data Protection Regulation ((EU) 2016/679) ("GDPR"); (iii) the Directive on Privacy and Electronic Communications (Directive 2002/58/EC), and (iv) any relevant United States federal and state data privacy laws, including the Electronic Communications Privacy Act, as amended ("ECPA") and the California Consumer Privacy Act of 2018, as amended ("CCPA");.

Data Recipient: means either party when it receives personal data from the other party in connection with the Contract;

IC: means the UK Information Commission;

EU Standard Contractual Clauses: means the contractual clauses annexed to the EU Commission Decision 2021/914/EU or any successor clauses approved by the EU Commission;

Permitted Jurisdiction: means a country or territory (a) in the case of any transfer from the EEA or the UK (unless otherwise stated by the UK government or the IC), in respect of which the European Commission has issued a finding of the adequacy of the protection of personal data; or (b) in the case of any transfer from the UK, which the UK Secretary of State has specified the standard of protection provided for data subjects with regard to the general processing of personal data is not materially lower than the standard required under UK law;

Permitted Recipients: means the parties to the Contract, the employees of each party and any third parties engaged to perform obligations in connection with the Contract;

Restricted Transfer: (i) where the GDPR applies, a transfer of personal data from the EEA either directly or via onward transfer, to any country or recipient outside of the EEA which is not a Permitted Jurisdiction; and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom either directly or via onward transfer, to any country or recipient outside of the UK which is not a Permitted Jurisdiction;

Restricted Transfer Terms: means the EU Standard Contractual Clauses and the UK SCC Addendum;

Shared Personal Data: has the meaning given in Condition 2.1;

Sub-processor: means a third party engaged by a processor (or any other Sub-processor) to carry out processing activities on behalf of the relevant controller;

UK Data Protection Legislation: means all applicable laws and regulations in the UK relating to the processing of personal data, including the UK GDPR and the Data Protection Act 2018;

UK-US Data Bridge: means the UK Extension to the EU-US Data Privacy Framework;

UK GDPR: means the GDPR as incorporated into UK law in accordance with the European Union (Withdrawal) Act 2018; and

UK SCC Addendum: means the International Data Transfer Addendum (IDTA) to the EU Standard Contractual Clauses issued by the IC.

2. Controller to Controller

2.1. The terms of this Condition 2 shall apply: (i) to the processing by either party of Business Contact Details disclosed by the other party in connection with the Contract; and (ii) to the extent that either party acts as a controller in relation to other personal data disclosed by the other party in connection with the Contract (such personal data together with any Business Contact Details processed under the Contract being "**Shared Personal Data**").

2.2. In relation to Shared Personal Data disclosed by the Data Discloser, the Data Recipient shall comply with all the obligations imposed on a controller under the Data Protection Legislation, and any material breach of the Data Protection Legislation by one party shall, if not remedied within 30 days of written notice from the other party, give grounds to the other party to terminate the Contract with immediate effect.

2.3. The Data Recipient shall process Business Contact Details disclosed by the Data Discloser for the Agreed Purpose only.

2.4. Each party shall:

2.4.1. ensure that it has satisfied a statutory ground under the Data Protection Legislation permitting it to transfer the Shared Personal Data to the Data Recipient and the Permitted Recipients (in the case of Business Contact Details, for the Agreed Purpose);

2.4.2. ensure that it has delivered to the data subjects such information as is required by Data Protection Legislation including the fact that the Data Discloser is sharing Shared Personal Data with the Data Recipient (or a category of recipients which includes the Data Recipient) and the purposes of the data transfer;

2.4.3. ensure that all Permitted Recipients are subject to written contractual obligations concerning the Shared Personal Data (including appropriate confidentiality and data security obligations); and

2.4.4. ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Shared Personal Data and against accidental loss or destruction of, or damage to, Shared Personal Data.

2.5. Each party shall assist the other in complying with all applicable requirements of the Data Protection Legislation relevant to Shared Personal Data processed in connection with the Contract. In particular, each party shall:

2.5.1. promptly inform the other party about the receipt of any data subject access request;

2.5.2. provide the other party with reasonable assistance, at the other party's cost, in complying with any data subject access request;

2.5.3. not disclose or release any Shared Personal Data in response to a data subject access request without first consulting the other party (to the extent possible and legally permitted), provided that such consultation shall not affect and be without prejudice to the party's ability to respond to the data subject access request within the time period required by Data Protection Legislation; and

2.5.4. notify the other party without undue delay on becoming aware of any breach of the Data Protection Legislation (providing such details as the other party may reasonably request).

2.6. The Data Discloser warrants that to the best of the Data Discloser's knowledge, the Shared Personal Data it discloses to the Data Recipient is accurate and up to date.

3. Controller to Processor

3.1. The terms of this Condition 3 shall apply to the extent that: (i) the Customer acts as a controller of personal data it discloses to the Supplier in connection with the Contract and the Supplier acts as a processor in relation to the personal data; or (ii) the Customer acts as a processor of personal data it discloses to the Supplier in connection with the Contract and the Supplier acts as a Sub-processor of the Customer in relation to the personal data.

3.2. Details of the: (i) subject-matter of the processing; (ii) duration of the processing; (iii) nature and purpose of the processing; (iv) categories of personal data; and (v) categories of data subject; for each Service can be found in the Data Sharing and Processing Agreement at: *https://www.qa.com/legal_documents/workforce-learning-data-sharing-and-processing-agreement.pdf* .

3.3. Supplier acknowledges that it shall only be a processor in respect of the personal data described in the Data Sharing and Processing Agreement at: *https://www.qa.com/legal_documents/workforce-learning-data-sharing-and-processing-agreement.pdf* and/or within the Contract.

3.4. The Supplier shall in relation to personal data that it processes on behalf of the Customer as a processor or Sub-processor:

3.4.1. process the personal data only on the documented instructions of the Customer as set out in the Contract or as otherwise notified to the

Supplier, unless required to do otherwise by Applicable Laws. If Supplier is of the opinion that any instruction given by the Customer breaches Data Protection Legislation, Supplier shall inform the Customer of this;

3.4.2. ensure that its personnel who are authorised to process data are under appropriate obligations of confidentiality;

3.4.3. implement appropriate technical and organisational measures in accordance with Article 32 of the GDPR or Article 32 of the UK GDPR (as applicable) in order to ensure an appropriate level of security for the personal data;

3.4.4. assist the Customer by implementing appropriate technical and organisational measures for the fulfilment of the Customer's obligation to respond to requests for exercising data subject rights;

3.4.5. provide assistance to the Customer in ensuring compliance with the Customer's obligations in Articles 32-36 of the GDPR or Articles 32-36 of the UK GDPR (as applicable), provided the Customer reimburses the reasonable costs incurred by the Supplier in providing such assistance;

3.4.6. upon request either: (i) destroy the personal data; or (ii) return the personal data to the Customer, upon termination or expiry of the Contract (subject to any legal obligation or internal retention policy that requires such personal data to be retained);

3.4.7. provide the Customer with such information as the Customer may reasonably request to demonstrate compliance with its obligations under this Condition 3; and

3.4.8. be entitled to make a Restricted Transfer: (i) where the recipient is located in a Permitted Jurisdiction; or (ii) the transfer is subject to the Restricted Transfer Terms; or (iii) in the case of Restricted Transfers to the United States, the Supplier maintains active certification under the Data Privacy Framework.

3.4.9. For the purposes of Condition 3.4.8 and 3.4.10 the Restricted Transfer Terms shall be deemed entered into (and incorporated into this Addendum by reference) and completed as follows:

EU Standard Contractual Clauses

(i) Module Two (Controller to Processor) shall apply where the Customer is a Controller of Shared Personal Data and the Supplier is processing Shared Personal Data;

(ii) Module Three (Processor to Processor) shall apply where the Customer is a Processor of Shared Personal Data and the Supplier is a sub-processor of Shared Personal Data;

(iii) Clause 7 of the EU Standard Contractual Clauses (Optional Docking Clause) shall not apply;

(iv) In Clause 9 of the EU Standard Contractual Clauses Option 2 shall apply and the time period for providing notice of a Sub-Processors shall be as specified in Condition 3.9;

(v) The Optional Language within Clause 11 of the EU Standard Contractual Clauses shall not apply;

(vi) In Clause 17 of the EU Standard Contractual Clauses Option 1 shall apply and the EU Standard Contractual Clauses shall be governed by Irish law;

(vii) In Clause 18(b) of the EU Standard Contractual Clauses disputes shall be dealt with by the courts of Ireland;

(viii) Annex I of the EU Standard Contractual Clauses shall be deemed completed with the information specified in the Data Sharing and Processing Agreement at *https://www.qa.com/legal_documents/workforce-learning-data-sharing-and-processing-agreement.pdf* and with any additional information provided on the Order;

(ix) Annex II of the EU Standard Contractual Clauses shall be deemed completed with the obligations specified in Condition 3.4.3, Appendix 2 and any additional information provided in the Order; and

(x) Annex III of the EU Standard Contractual Clauses shall be deemed completed with the information specified in the Data Sharing and Processing Agreement at *https://www.qa.com/legal_documents/workforce-learning-data-sharing-and-processing-agreement.pdf* and with any additional information provided in the Order.

3.4.10. The parties agree that the Supplier shall be entitled to make a Restricted Transfer:

3.4.10.1. utilising the UK-US Data-Bridge provided that (i) the Supplier maintains active certification under the DPF including the UK Extension; (ii) the Supplier Processes Personal Data in compliance with the DPF Principles; (iii) any recipient of Personal Data is self-certified under the UK-US Data Bridge and listed on the Data Privacy Framework list maintained by the U.S. Department of Commerce; and (iv) the Supplier promptly notifies the Customer if its certification lapses or is withdrawn;

3.4.10.2. utilising the UK SCC Addendum and the UK SCC Addendum shall be deemed entered into (and incorporated into this Addendum by reference), as set out in Appendix 1 of this Addendum.

3.4.11. In the event that any provision of this Addendum contradicts directly or indirectly with the EU Standard Contractual Clauses or the UK SCC Addendum, the provisions of the applicable EU Standard Contractual Clauses or the UK SCC Addendum shall prevail over the terms of the Addendum.

3.4.12. The Supplier shall notify the Customer without undue delay (and in any event within 48 hours) on becoming aware of any breach of the Data Protection Legislation.

3.5. If Supplier is located outside the UK or the EEA but not in a Permitted Jurisdiction, Restricted Transfers shall be subject to (i) the UK-US Data-Bridge; or (ii) the Restricted Transfer Terms shall govern the transfer of personal data by the Customer to Supplier under the Contract and the Customer and Supplier agree to be bound by the Restricted Transfer Terms as data exporter and data importer respectively.

3.6. The Customer consents to the use by the Supplier of the Sub-Processors detailed in the Data Sharing and Processing Agreement at *https://www.qa.com/legal_documents/workforce-learning-data-sharing-and-processing-agreement.pdf* .

3.7. The Customer gives general authorisation to the Supplier to engage additional Sub-processors under the conditions set forth below and Supplier shall:

3.7.1. require its Sub-Processors to enter into a written agreement on substantially the same terms as those set out in this Condition 3;

3.7.2. remain fully liable to the Customer for the performance of its Sub-Processors' obligations;

3.8. provide a list of its Sub-Processors to the Customer upon request; and

3.9. inform the Customer, prior to the appointment of a new Sub-Processor, so as to give the Customer an opportunity to object to the change. If the Customer does not notify Supplier that it objects to the appointment of a new Sub-Processor within fourteen (14) days of Supplier's notice of the proposed appointment, the Customer will be deemed to have accepted the appointment. The parties shall discuss any objections raised by the Customer in good faith. Notification of new Sub-Processors by Supplier will be made by way of update to the Data Sharing and Processing Agreement at *https://www.qa.com/legal_documents/workforce-learning-data-sharing-and-processing-agreement.pdf* and where applicable notification shall be made by way of a service delivery message to the Customer.

3.10. Sub-Processors may make Restricted Transfers of personal data for the purpose of providing the Services to the Customer in accordance with the Contract. The Supplier shall ensure that such Sub-Processors: (i) are located in a Permitted Jurisdiction; or (ii) have entered into the applicable Restricted Transfer Terms with the Supplier.

Appendix 1

UK STANDARD CONTRACTUAL CLAUSES ADDENDUM

1. This Appendix 1 hereby incorporates Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the IC and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18 of those Mandatory Clauses.

2. The following tables set out the information required by Part 1 of the Approved Addendum:

Start date	commencement of the Contract	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: As set out in the Order Trading name (if different): N/A Main address (if a company registered address): As set out in the Order Official registration number (if any) (company number or similar identifier): As set out in the Order	Full legal name: As set out in the Order Trading name (if different): N/A unless specified on the Order Main address (if a company registered address): As set out in the Order Official registration number (if any) (company number or similar identifier): As set out in the Order
Key Contact	Full Name (optional): As set out in the Order Job Title: As set out in the Order Contact details including email: As set out in the Order	Full Name (optional): As set out in the Order Job Title: As set out in the Order Contact details including email: As set out in the Order
Signature (if required for the purposes of Section 2)	The Exporter confirms agreement to be bound by this UK Standard Contractual Clauses Addendum by signing the Order.	The Importer confirms agreement to be bound by this UK Standard Contractual Clauses Addendum by signing the Order.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCC	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum: N/A

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As specified on the Order
Annex 1B: Description of Transfer: See Data Sharing and Processing Agreement at: *https://www.qa.com/legal_documents/workforce-learning-data-sharing-and-processing-agreement.pdf*

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: The Supplier will implement appropriate technical and organisational measures in accordance with Appendix 2 and any additional terms specified on the Order.
Annex III: List of Sub processors (Modules 2 and 3 only): See Data Sharing and Processing Agreement at: *https://www.qa.com/legal_documents/workforce-learning-data-sharing-and-processing-agreement.pdf*

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ neither Party

Appendix 2
Information Security

1. **INFORMATION SECURITY**

1.1. The Supplier shall:

1.1.1. have in place an information security policy which covers the scope of the Services and meets ISO27001 standards (the "**Security Policy**");

1.1.2. ensure the Security Policy is reviewed at least annually by the Supplier and communicated to all relevant staff and/or contractors;

1.1.3. procure the maintenance of independent external security certifications and assurances, including ISO27001, Cyber Essentials Plus, and the UK Government's IT Health Check ('CHECK') scheme;

1.1.4. have a documented IT asset disposal policy; and

1.1.5. have in place an acceptable use policy for the use of Supplier systems including email and internet; such policy shall cover misuse of resources and the downloading and installing of unauthorised software.

1.2. The Supplier shall ensure it maintains sufficient resources, skills and facilities to meet its responsibilities under this Appendix.

2. **RECORDS, AUDIT AND NOTIFICATIONS**

2.1. The Supplier shall:

2.1.1. conduct internal and external audits of its security controls and the Security Policy;

2.1.2. provide independent third-party audit reports to Customer (such reports are at the Supplier's discretion and may be a summary or redacted reports); and

2.1.3. notify the Customer promptly of becoming aware of any incident that has materially impacted the security of the Customer's information or data.

3. **DATA DELETION**

3.1. The Supplier shall ensure:

3.1.1. it has the ability to sanitize computing resources of data at an appropriate time; and

3.1.2. it has processes and procedures in place for the secure deletion of Customer data upon request by the Customer.

4. **DATA ACCESS**

4.1. The Supplier shall ensure that people that are not directly involved in the provision of the Services or who do not have a legitimate need to access Customer Data shall not have unsupervised access to the Customer Data or systems involved in the provision of Services to the Customer.

4.2. The Supplier shall have in place systems and processes for individuals which may have access to Customer data or information.

4.3. The Supplier shall review all system users' and administrators' access rights to Customer and Supplier data at reasonable intervals.

5. **SECURITY**

5.1. Throughout the Term the Supplier shall take appropriate measures to guard against unauthorised or unlawful processing of Customer data and against accidental corruption, loss or destruction of or damage to Customer data.

5.2. The Supplier shall have appropriate operational security risk management processes and procedures in place for the identification, mitigation and management of security risks as they pertain to the Services.

5.3. The Supplier shall have in place systems and tools to protect Customer data and information from malicious attack.

5.4. The Supplier shall ensure it has appropriate information security protection in place for all locations processing Customer Data, as set forth by applicable legislation, regulations, and industry best practice.

6. **INCIDENT MANAGEMENT**

6.1. The Supplier shall:

6.1.1. have in place a robust security incident management policy which is implemented upon the occurrence of any security incident or risk;

6.1.2. without undue delay notify the Customer of any security incident relating to Customer data;

6.1.3. provide Customer with such information Customer reasonably requires to understand the scale and scope of any relevant security incident and to remediate its impact;

6.1.4. deal with any security incident in accordance with good industry standards;

6.1.5. have in place appropriate business continuity plans to ensure, so far as is reasonably practicable, the continuity of the Services despite any security incident;

6.1.6. ensure that Customer data is appropriately backed up and is capable of restoration upon loss or damage; and

6.1.7. ensure all back up data is appropriately stored to the same standards as other data.

7. **CHANGES**

7.1. The Customer acknowledges that the Supplier may be required to update this Addendum from time to time to deal with changes in Applicable Laws, any new security threats or a change in the Customer's or the Supplier's business and as such the Supplier agrees to comply with any updated version of this Addendum from time to time