

Contract (Short Form – Services)

Contract for the provision of a call off facility of training modules for First-Level and Mid-Level Leadership

Contract Reference CQC RCCO 083

1st September 2023

Contents

1	Interpretation.....	2
2	Priority of documents	10
3	Supply of Services	10
4	Term	11
5	Price, Payment and Recovery of Sums Due.....	12
6	Premises and equipment	13
7	Staff and Key Personnel	14
8	Assignment and sub-contracting.....	15
9	Intellectual Property Rights	16
10	Governance and Records.....	18
11	Confidentiality, Transparency and Publicity	18
12	Freedom of Information	20
13	Protection of Data.....	20
13A	Security	22
14	Liability and Insurance	22
15	Force Majeure	24
16	Termination	24
17	Compliance	25
18	Prevention of Fraud, Corruption and Bribery	26
19	Dispute Resolution	27
20	General.....	27
21	Notices	29
22	Governing Law and Jurisdiction	30
23	TUPE	30

SCHEDULE 1 –SPECIFICATION32

SCHEDULE 2 – PRICE34

SCHEDULE 3 – Contractor’s RESPONSE36

SCHEDULE 4 – PROCESSING, PERSONAL DATA AND DATA SUBJECTS38

SCHEDULE 5 – SECURITY REQUIREMENTS AND PLAN81

SCHEDULE 6 – CHANGE CONTROL90

SCHEDULE 7 – THIRD PARTY SOFTWARE (NOT USED).....91

SCHEDULE 8 – EXIT MANAGEMENT STRATEGY92

THIS CONTRACT is dated 1st September 2023

PARTIES

- (1) **CARE QUALITY COMMISSION** of Citygate Gallowgate Newcastle upon Tyne NE1 4PA (“**Authority**”)

and

- (2) **DEVELOPMENT DIMENSIONS INTERNATIONAL (UK) LTD**, (Company Number 01683848), located at the Connection, 198 High Holborn, London, WC1V 7BD, UNITED KINGDOM (“**Contractor**”)

(Together the “**Parties**”)

Background

1. The Authority is the independent health and social care regulator in England that monitors, inspects and regulates health and social care services to ensure they meet fundamental standards of quality and safety. It ensures health and social care services provide people with safe, effective, compassionate, high-quality care and we encourage care services to improve. In 2021 CQC published a new strategy for the changing world of health and social care. The strategy aims to make our regulation more relevant to the way care is now delivered, more flexible to manage risk and uncertainty, and it will enable CQC to respond in a quicker and more proportionate way as the health and care environment continues to evolve.
2. The Academy is the CQC’s learning and development department offering a range of developmental courses and programmes for all colleagues. As part of its strategy to grow capability among its leaders and managers it has a suite of leadership resources including ‘The Successful Manager’. This programme is made up of facilitated learning events using learning resources.
3. This Contract will facilitate line managers access to various training modules via CQC’s Learning Management System (LMS) ED whereby the CQC Trainers will deliver virtual training classes. Modules to be accessed by individuals on a call off basis.
4. The Contractor has been appointed by the Authority to provide the Services.
5. Therefore, the Parties have agreed to enter into this Contract for the provision of the services defined in the Specifications.

1 Interpretation

“Agreement”	means this Contract
“Approval”	means the written consent of the Authority;
“Authority”	means the Care Quality Commission. Authority is also referred to at times herein as “Controller”;
“Authority Data”	<p>means:</p> <ul style="list-style-type: none">(a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Contractor by or on behalf of the Authority; or (ii) which the Contractor is required to generate, process, store or transmit pursuant to the Contract; or(b) any Personal Data for which the Authority is the Data Controller;
“Anti-Slavery and Human Trafficking Laws”	means all applicable anti-slavery and human trafficking laws, statutes, regulations, policies and codes from time to time in force including but not limited to the Modern Slavery Act 2015;
“Breach of Security”	means the occurrence of unauthorised access to or use of the Premises, the Premises, the Services, the Contractor system, or any ICT (as defined in Schedule 5 (Security Requirements) or data (including Authority Data) used by the Authority or the Contractor in connection with the Contract;
“Central Government Body”	<p>means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:</p> <ul style="list-style-type: none">(a) Government Department;(b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);(c) Non-Ministerial Department; or

(d) Executive Agency;

“Change Control Notice (“CCN”)”	means a change control notice in the form set out in Schedule 6;
“Commencement Date”	means the date of commencement of the Contract which is 1 st September 2023;
“Contract”	means the contract consisting of these terms and conditions, any attached Schedules, the Specification, the Contractor’s Response and the Pricing Schedule;
“Confidential Information”	means all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (i) is known by the receiving Party to be confidential; (ii) is marked as or stated to be confidential; or (iii) ought reasonably to be considered by the receiving Party to be confidential;
“Contractor”	means the person named as Contractor who was awarded this Contract. Contractor is also referred to at times herein as “Processor”;
“Contractor’s Response”	means the document submitted by the Contractor to the Authority in response to the Authority’s invitation to suppliers for formal offers to supply the Services appended hereto in Schedule 3;
“Contractor System”	means the information and communications technology system used by the Contractor in performing the Services including the Tools (as defined at section 9), Software (if any, as defined in Schedule 5 (Security Requirements), the Contractor Equipment (if any, as defined in Schedule 5 (Security Requirements) and related cabling (but excluding the Authority System);

“Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Data Protection Officer”	shall each have the same meaning given in the UK GDPR ;
“Data Protection Legislation	means (i) all applicable UK law relating to the processing of personal data and privacy, including but not limited to the UK GDPR, and the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy; and (ii) (to the extent that it may be applicable) the EU GDPR). The UK GDPR and EU GDPR are defined in section 3 of the Data Protection Act 2018;
“Data Loss Event”	means any event that results, or reasonably may result, in unauthorised access to Personal Data held by the Processor under this Contract and/or actual or reasonably potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;
“Data Protection Impact Assessment”	means an assessment by the Controller carried out in accordance with Section 3 of the UK GDPR and sections 64 and 65 of the DPA 2018;
“Data Subject Request”	means a request made by or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
“DPA 2018”	means the Data Protection Act 2018;
“Default”	means any breach of the obligations of the relevant Party (including abandonment of the Contract in breach of its terms, repudiatory breach or breach of a fundamental term) or any other default, act, omission, negligence or statement of the relevant Party or the Staff in connection with the subject-matter of the Contract and in respect of which such Party is liable to the other;
“Expiry Date”	means the date for expiry of the Contract which is 31 st August 2024;

“Extended Period”	means the period by which the term of this contract may be extended.
“FOIA”	means the Freedom of Information Act 2000;
“Good Industry Practice”	means standards, practices, methods and procedures conforming to the Law and the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar type of undertaking under the same or similar circumstances;
“Information”	has the meaning given under section 84 of the FOIA;
“IDTA”	means the International Data Transfer Agreement found at Schedule 4 Annex 2 of the Contract ;
“Key Personnel”	means any persons specified as such in the Specification or Contract otherwise notified as such by the Authority to the Contractor in writing;
“Law”	means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgement of a relevant court of law, or directives or requirements with which the Processor is bound to comply;
“Loss”	means any losses, costs, price, expenses, interest, fees (including reasonable legal fees), payments, demands, liabilities, claims, proceedings, actions, penalties, price, fines, damages, destruction, adverse judgments, orders or other sanctions and the term “Losses” shall be construed accordingly;
“Module Cost”	means the price for a specific Module as set out in Schedule 2
“Module”	means the services offered by the Contractor in response to the Specification under this Contract as set out in Schedule 2
“Party”	means the Contractor or the Authority (as appropriate) and “Parties” shall mean both of them;

“Premises”	means the location where the Services are to be supplied, as set out in the Specification;
“Price”	means the price (excluding any applicable VAT) payable to the Contractor by the Authority as set out in Schedule 2.
“Price Cap”	means the maximum total value of the Contract which is £60,000
Pricing Schedule”	means Schedule 3 containing details of the Price;
“Processing”	has the meaning given to it in the Data Protection Legislation but, for the purposes of the Contract, it shall include both manual and automatic processing and "Process" and "Processed" shall be interpreted accordingly;
“Processor Personnel”	means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor and/or any Sub-Processor engaged in the performance of its obligations under this Contract;
“Prohibited Act”	<p>means:</p> <ul style="list-style-type: none"> (a) to directly or indirectly offer, promise or give any person working for or engaged by the Authority a financial or other advantage to: <ul style="list-style-type: none"> induce that person to perform improperly a relevant function or activity; or reward that person for improper performance of a relevant function or activity; (b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with the Contract; (c) an offence: <ul style="list-style-type: none"> i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act; ii) under legislation or common law concerning fraudulent acts; or iii) the defrauding, attempting to defraud or conspiring to defraud the Authority;

any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct has been carried out in the UK;

“Protective Measures”	means appropriate technical and organisational measures designed to ensure compliance with obligations of the Parties arising under Data Protection Legislation and this Contract, which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Schedule 5 (Security Requirements and Plan);
“Purchase Order Number”	means the Authority’s unique number relating to the supply of the Services by the Contractor to the Authority in accordance with the terms of the Contract;
“Relevant Requirements”	means all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State for Justice pursuant to section 9 of the Bribery Act 2010;
“Replacement Contractor”	means any third party supplier appointed by the Authority to supply any services which are substantially similar to any of the Services in substitution for any of the Services following the expiry, termination or partial termination of the Contract;
“Request for Information”	has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term “request” shall apply);
“Schedule”	means a schedule attached to, and forming part of, the Contract;
“Security Plan”	means the Contractor’s security plan prepared pursuant to paragraph 3 of Schedule 5 (Security Requirements and Plan), an outline of which is set out in an Appendix to Schedule 5;
“Security Framework”	Policy means the HMG Security Policy Framework (https://www.gov.uk/government/publications/security-policy-framework)
“Services”	means the services to be supplied by the Contractor to the Authority under the Contract as set out in Schedule 1

“Specification”	means the specification for the Services (including as to quantity, description and quality) as specified in the in Schedule 1;
“Staff”	means all directors, officers, employees, agents, consultants and contractors of the Contractor and/or of any Sub-contractor of the Contractor engaged in the performance of the Contractor’s obligations under the Contract;
“Staff Vetting Procedures”	means vetting procedures that accord with Good Industry Practice or, where requested by the Authority, the Authority’s procedures for the vetting of personnel as provided to the Contractor from time to time;
“Sub–Contractor”	means a third party directly or indirectly contracted to the Contractor (irrespective of whether such person is an agent or company within the same group of companies as the Contractor) whose services are used by the Contractor (either directly or indirectly) in connection with the provision of the Services, and “Sub-Contract” shall be construed accordingly;
“Sub-processor”	means any third Party appointed to process Personal Data on behalf of the Processor related to this Contract;
“Supplier Code of Conduct”	means the HM Government Supplier Code of Conduct v2 dated February 2019
“Term”	means the period from the Commencement Date to the Expiry Date and such period may be extended in accordance with clause 4.2 or terminated in accordance with the terms and conditions of the Contract;
“Third Party Software”	means software which is proprietary to any third party which is or will be used by the Contractor to provide the Services including the software and which is specified as such in Schedule 7;
“TUPE”	means the Transfer of Undertakings (Protection of Employment) Regulations 2006;
“UK GDPR”	means the UK General Data Protection Regulation;
“VAT”	means value added tax in accordance with the provisions of the Value Added Tax Act 1994; and
“Variation”	means a variation to the Specification, the Price or any of the terms and conditions of the Contract;

“Working Day”

means a day (other than a Saturday or Sunday) on which banks are open for business in the City of London.

- 1.1 In these terms and conditions, unless the context otherwise requires:
- 1.2.1 references to numbered clauses are references to the relevant clause in these terms and conditions;
 - 1.2.2 any obligation on any Party not to do or omit to do anything shall include an obligation not to allow that thing to be done or omitted to be done;
 - 1.2.3 the headings to the clauses of these terms and conditions are for information only and do not affect the interpretation of the Contract;
 - 1.2.4 any reference to an enactment includes reference to that enactment as amended or replaced from time to time and to any subordinate legislation or byelaw made under that enactment; and
 - 1.2.5 the word 'including' shall be understood as meaning 'including without limitation'.

2 Priority of documents

- 2.1 In the event of, and only to the extent of, any conflict between the clauses of the Contract, any document referred to in those clauses and the Schedules, the conflict shall be resolved in accordance with the following order of precedence:
- a) these terms and conditions
 - b) Schedule 1 (Specification);
 - c) Schedule 2 (Price);
 - d) the remaining Schedules; and
 - c) any other document referred to in these terms and conditions

3 Supply of Services

- 3.1 In consideration of the Authority's agreement to pay the Price, the Contractor shall supply the Services to the Authority for the Term subject to and in accordance with the terms and conditions of this Contract.
- 3.2 The Authority's authorised officer may place orders for Modules as set out in Schedule 2. The Contractor will in turn provide the services relevant to the Module once the order has been placed.
- 3.3 For the avoidance of doubt, no Module is guaranteed to be ordered by the Authority.
- 3.4 In supplying the Services, the Contractor shall:
- 3.2.1 co-operate with the Authority in all matters relating to the Services and comply with all the Authority's reasonable instructions;

- 3.2.2 perform the Services with all reasonable care, skill and diligence in accordance with Good Industry Practice in the Contractor's industry, profession or trade;
 - 3.2.3 use Staff who are suitably skilled, experienced and possess the required qualifications to perform tasks assigned to them, and in sufficient number to ensure that the Contractor's obligations are fulfilled in accordance with the Contract;
 - 3.2.4 ensure that the Services shall conform with all descriptions and specifications set out in the Specification;
 - 3.2.5 comply with all applicable Laws; and
 - 3.2.6 provide all equipment, tools and vehicles and other items as are required to provide the Services.
- 3.5 The Authority may by written notice to the Contractor at any time request a Variation to the scope of the Services. If the Contractor agrees to any Variation to the scope of the Services, the Price shall be subject to fair and reasonable adjustment to be agreed in writing between the Authority and the Contractor.
- 3.6 Any Variation will not take effect unless recorded in a Change Control Notice in the form set out in Schedule 6 and approved in writing by the Parties.
- 3.7 As part of the Services, the Contractor Staff certified as trainers ("**Contractor Trainers**") or Authority employees trained and certified by the Contractor as trainers ("**Authority Trainers**") may perform workshops ("**Contractor Workshops**") for Participants. The Authority may also have Authority employees trained as Master Trainers, and such Master Trainers may certify additional employees as Authority Trainers. No other Staff are authorized to perform Contractor Workshops. Authority Trainers and Authority Master Trainers may only perform Contractor Workshops as previously agreed with the Contractor.

4 Term

- 4.1 The Contract shall take effect on the Commencement Date and shall expire on the Expiry Date.

5 Price, Payment and Recovery of Sums Due

- 5.1 The Price for the Services shall be based on the Module Costs set out in Schedule 2. The Module Costs as set out in in Schedule 2 shall be the full and exclusive remuneration of the Contractor in respect of the supply of each Module. Unless otherwise agreed in writing by the Authority, the Price shall include every cost and expense of the Contractor directly or indirectly incurred in connection with the performance of the Services. The maximum total price payable by the Authority under this Contract shall not exceed the Price Cap.

- 5.2 The Contractor shall invoice the Authority as specified in Schedule 2. Each invoice shall include such supporting information required by the Authority to verify the accuracy of the invoice, including the relevant Purchase Order Number and a breakdown of the Services supplied in the invoice period.
- 5.3 In consideration of the supply of the Services by the Contractor, the Authority shall pay the Contractor the invoiced amounts no later than 30 days after receipt of a valid invoice which includes a valid Purchase Order Number. The Authority may, without prejudice to any other rights and remedies under the Contract, withhold or reduce payments in the event of unsatisfactory performance.
- 5.4 All amounts stated are exclusive of VAT which shall be charged at the prevailing rate. The Authority shall, following the receipt of a valid VAT invoice, pay to the Contractor a sum equal to the VAT chargeable in respect of the Services.
- 5.5 If there is a dispute between the Parties as to the amount invoiced, the Authority shall pay the undisputed amount. The Contractor shall not suspend the supply of the Services unless the Contractor is entitled to terminate the Contract for a failure to pay undisputed sums in accordance with clause 16.4. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause 19.
- 5.6 If a payment of an undisputed amount is not made by the Authority by the due date, then the Authority shall pay the Contractor interest at the interest rate specified in the Late Payment of Commercial Debts (Interest) Act 1998.
- 5.7 If any sum of money is recoverable from or payable by the Contractor under the Contract (including any sum which the Contractor is liable to pay to the Authority in respect of any breach of the Contract), that sum may be deducted unilaterally by the Authority from any sum then due, or which may come due, to the Contractor under the Contract or under any other agreement or contract with the Authority. The Contractor shall not be entitled to assert any credit, set-off or counterclaim against the Authority in order to justify withholding payment of any such amount in whole or in part.
- 5.8 Where the Contractor enters into a sub-contract, the Contractor shall include in that sub-contract:
- 5.8.1 Provisions having the same effect as clauses 5.2 to 5.6 of the Contract and
- 5.8.2 Provisions requiring the counterparty to that subcontract to include in any sub-contract which it awards provisions having the same effect as clauses 5.2 to 5.6 of this Contract.
- 5.8.3 In this clause 5.8 'sub-contract' means a contract between two or more Contractors, at any stage of remoteness from the Authority in a sub-contracting chain, made wholly or substantially for the purpose of performing (or contributing to the performance of) the whole or any part of this Contract.

6 Premises and equipment

- 6.1 If necessary, the Authority shall provide the Contractor with reasonable access at reasonable times to its premises for the purpose of supplying the Services. All equipment, tools and vehicles brought onto the Authority's premises by the Contractor or the Staff shall be at the Contractor's risk.
- 6.2 If the Contractor supplies all or any of the Services at or from the Authority's premises, on completion of the Services or termination or expiry of the Contract (whichever is the earlier) the Contractor shall vacate the Authority's premises, remove the Contractor's plant, equipment and unused materials and all rubbish arising out of the provision of the Services and leave the Authority's premises in a clean, safe and tidy condition. The Contractor shall be solely responsible for making good any damage to the Authority's premises or any objects contained on the Authority's premises which is caused by the Contractor or any Staff, other than fair wear and tear.
- 6.3 If the Contractor supplies all or any of the Services at or from its premises or the premises of a third party, the Authority may, during normal business hours and on reasonable notice, inspect and examine the manner in which the relevant Services are supplied at or from the relevant premises.
- 6.4 The Authority shall be responsible for maintaining the security of its premises in accordance with its standard security requirements. While on the Authority's premises the Contractor shall, and shall procure that all Staff shall, comply with all the Authority's security requirements.
- 6.5 Where all or any of the Services are supplied from the Contractor's premises, the Contractor shall, at its own cost, comply with all reasonable and appropriate security requirements specified by the Authority in writing.
- 6.6 Without prejudice to clause 3.2.6, any equipment provided by the Authority for the purposes of the Contract shall remain the property of the Authority and shall be used by the Contractor and the Staff only for the purpose of carrying out the Contract. Such equipment shall be returned promptly to the Authority on expiry or termination of the Contract.
- 6.7 The Contractor shall reimburse the Authority for any loss or damage to the equipment (other than deterioration resulting from normal and proper use) caused by the Contractor or any Staff. Equipment supplied by the Authority shall be deemed to be in a good condition when received by the Contractor or relevant Staff unless the Authority is notified otherwise in writing within 5 Working Days.
- 6.8 Any Premises/land made available from time to time to the Contractor by the Authority in connection with the Contract, shall be made available to the Contractor on a non-exclusive licence basis free of charge and shall be used by the Contractor solely for the purpose of performing its obligations under the Contract. The Contractor shall have the use of such Premises/land as licensee and shall vacate the same on completion, termination or abandonment of the Contract.

- 6.9 The Parties agree that there is no intention on the part of the Authority to create a tenancy of any nature whatsoever in favour of the Contractor or its Staff and that no such tenancy has or shall come into being and, notwithstanding any rights granted pursuant to the Contract, the Authority retains the right at any time to use any premises owned or occupied by it in any manner it sees fit.
- 6.10 Should the Contractor require modifications to the Premises, such modifications shall be subject to prior Approval and shall be carried out by the Authority at the Contractor's expense. The Authority shall undertake approved modification work without undue delay. Ownership of such modifications shall rest with the Authority.
- 6.11 All the Contractor's equipment shall remain at the sole risk and responsibility of the Contractor, except that the Authority shall be liable for loss of or damage to any of the Contractor's property located on Authority's premises which is due to the negligent act or omission of the Authority.

7 Staff and Key Personnel - NOT USED

- 7.1 If the Authority reasonably believes that any of the Staff are unsuitable to undertake work in respect of the Contract, it may, by giving written notice to the Contractor:
- 7.1.1 refuse admission to the relevant person(s) to the Authority's premises;
 - 7.1.2 direct the Contractor to end the involvement in the provision of the Services of the relevant person(s); and/or
 - 7.1.3 require that the Contractor replace any person removed under this clause with another suitably qualified person and procure that any security pass issued by the Authority to the person removed is surrendered,
- and the Contractor shall comply with any such notice.
- 7.2 The Contractor shall:
- 11.2.4 ensure that all Staff are vetted in accordance with the Staff Vetting Procedures; and if requested, comply with the Authority's Staff Vetting Procedures as supplied from time to time;
 - 11.2.4 if requested, provide the Authority with a list of the names and addresses (and any other relevant information) of all persons who may require admission to the Authority's premises in connection with the Contract;
 - 11.2.4 procure that all Staff comply with any rules, regulations and requirements reasonably specified by the Authority; and
 - 11.2.4 shall at all times comply with the Supplier Code of Conduct (<https://www.gov.uk/government/publications/Contractor-code-of-conduct>).

- 11.2.4 ensure that it does not engage in any act or omission that would contravene Anti-Slavery and Human Trafficking Laws.
- 7.3 Any Key Personnel shall not be released from supplying the Services without the agreement of the Authority, except by reason of long-term sickness, maternity leave, paternity leave, termination of employment or other extenuating circumstances.
- 7.4 Any replacements to the Key Personnel shall be subject to the prior written agreement of the Authority (not to be unreasonably withheld). Such replacements shall be of at least equal status or of equivalent experience and skills to the Key Personnel being replaced and be suitable for the responsibilities of that person in relation to the Services.
- 7.5 At the Authority's written request, the Contractor shall provide a list of names and addresses of all persons who may require admission in connection with the Contract to the Premises, specifying the capacities in which they are concerned with the Contract and giving such other particulars as the Authority may reasonably request.
- 7.6 The Contractor's Staff, engaged within the boundaries of the Premises shall comply with such rules, regulations and requirements (including those relating to security arrangements) as may be in force from time to time for the conduct of personnel when at or outside the Premises.
- 7.7 The Authority may require the Contractor to ensure that any person employed in the provision of the Services has undertaken a Disclosure and Barring Service check as per the Staff Vetting Procedures.

8 Assignment and sub-contracting

- 8.1 The Contractor shall not without the written consent of the Authority assign, sub-contract, novate or in any way dispose of the benefit and/ or the burden of the Contract or any part of the Contract. The Authority may, in the granting of such consent, provide for additional terms and conditions relating to such assignment, sub-contract, novation or disposal. The Contractor shall be responsible for the acts and omissions of its Sub-contractors as though those acts, and omissions were its own.
- 8.2 If the Contractor enters into a Sub-Contract for the purpose of performing its obligations under the Contract, it shall ensure that a provision is included in such sub-contract which requires payment to be made of all sums due by the Contractor to the Sub-Contractor within a specified period not exceeding 30 days from the receipt of a valid invoice.
- 8.3 If the Authority has consented to the placing of Sub-Contracts, the Contractor shall:
- (a) impose obligations on its Sub-Contractor on the same terms as those imposed on it pursuant to this Contract and shall procure that the Sub-Contractor complies with such terms; and

- (b) provide a copy at no charge to the Authority, of any Sub-Contract, on receipt of a request for such by the Authority.
- 8.4 The Authority may assign, novate, or otherwise dispose of its rights and obligations under the Contract with notice to Contractor, but without the consent of the Contractor provided that such assignment, novation or disposal shall not increase the burden of the Contractor's obligations under the Contract.

9 Intellectual Property Rights

- 9.1 For the purposes of this Agreement and clause 9, "Materials" means all copyright-protected or copyrightable products and the content thereof provided to the Authority by the Contractor, including but not limited to competencies, workbooks, training aids, slides, business drivers, development guides, interview questions information, and learning materials provided to the Participants (as defined below) and training facilitators, regardless of the format.
- 9.2 All intellectual property rights in any materials provided by the Authority to the Contractor for the purposes of this Contract shall remain the property of the Authority but the Authority hereby grants the Contractor a royalty-free, non-exclusive and non-transferable licence to use such materials as required until termination or expiry of the Contract for the sole purpose of enabling the Contractor to perform its obligations under the Contract.
- 9.3 All intellectual property rights in any usage statistics, reports, scores and results generated from the Authority's authorised use of the Contractor's Tools (as defined below) (collectively "Results") shall vest in the Authority. For the avoidance of doubt, Results shall not include the design, form or format of reports, or any Contractor Materials including content or competencies contained within a report. If, and to the extent, that any intellectual property rights in such Results vest in the Contractor by operation of law, the Contractor hereby assigns to the Authority by way of a present assignment of future rights that shall take place immediately on the coming into existence of any such intellectual property rights all its intellectual property rights in such Results (with full title guarantee and free from all third party rights).
- 9.4 The Authority hereby grants the Contractor:
 - 9.3.1 a royalty – free non-exclusive license to use all intellectual property rights in the Results in anonymized and aggregated form for the Contractors statistical norming, research and development purposes until termination or expiry of the Contract. When used for these purposes, these Results will not be personally identifiable, nor will such information be aggregated in such a way as to compromise the anonymity of the Authority employees who participate in the Services ("Participants"). Except as otherwise authorized above, the Contractor will not use the Results for Commercial purposes.

- 9.5 The Contractor shall retain all right, title, and interest in and to all Materials. The Contractor provides the Authority a non-exclusive, non-transferable, non-sublicensable, worldwide license to use the Materials solely for the Authority's internal business purposes. The Authority shall have no right to modify, translate, or copy such Materials, unless such a right is previously provided in writing by the Contractor. The Contractor will retain copyrights on all modified, copied, and translated Materials. Electronic Materials and/or hard copy Materials are not returnable for refund.

9.4.1 The Parties agree that:

- a) access to such Materials is restricted to Participants in the course for which the Materials were provided;
- b) each Participant may print one set of such Materials for personal use during and after attending the specified virtual or in person classroom;
- c) the Authority shall send monthly reports to the Contractor certifying usage of Materials only on months where orders for Modules have been placed by the Authority;
- d) the period of use of any electronic master file of Materials shall be coterminous with the applicable Module ; and
- e) upon termination of the Contract the Authority agrees not to reproduce the Materials or retain any copies for circulation and delete any electronic or digital versions of the Materials. The Authority shall at the request of the Contractor confirm destruction of such electronic or digital versions of the Materials to the Contractor in writing following the expiry or termination of the Contract.

9.4.2. Technology Services. Web-based or Cloud-based applications, virtual reality programs, equipment, assessments, testing, software systems and related tools which may be used by the Contractor to perform and provide the Services ("**Tools**") will reside on computer equipment within the United States, with security provisions commensurate with this Agreement. These Tools are the property of the Contractor or have been licensed by the Contractor, and Contractor retains all rights to such. Contractor shall retain all right, title, and interest in and to all Tools. The Contractor provides the Authority a non-exclusive, non-transferable, non-sublicensable, worldwide license to use the Tools solely for the Authority's internal business purposes.

- 9.6 The Contractor shall indemnify, and keep indemnified, the Authority in full against all costs, expenses, damages and losses (whether direct or indirect), including any interest, penalties, and reasonable legal and other professional fees awarded against or incurred or paid by the Authority as a result of or in connection with any claim made against the Authority for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Services, to the extent that the claim is attributable to the acts or omission of the Contractor its Staff, agents or Sub-contractors.

- 9.7 The Authority shall promptly notify the Contractor of any infringement claim made against it relating to any Services and, subject to any statutory obligation requiring the Authority to respond, shall permit the Contractor to have the right, at its sole discretion to assume, defend, settle or otherwise dispose of such claim. The Authority shall give the Contractor such assistance as it may reasonably require to dispose of the claim and shall not make any statement which might be prejudicial to the settlement or defence of the claim.

10 Governance and Records

- 10.1 The Contractor shall:
- 10.1.1 attend progress meetings with the Authority at the frequency and times specified by the Authority and shall ensure that its representatives are suitably qualified to attend such meetings; and
 - 10.1.2 submit progress reports to the Authority at the times and in the format specified by the Authority.
- 10.2 The Contractor shall keep and maintain until 6 years after the end of the Contract, or as long a period as may be agreed between the Parties, full and accurate records of the Contract including the Services supplied under it and all payments made by the Authority. The Contractor shall on request afford the Authority or the Authority's representatives such access to those records as may be reasonably requested by the Authority in connection with the Contract.

11 Confidentiality, Transparency and Publicity

- 11.1 Subject to clause 11.2, each Party shall:
- 11.1.1 treat all Confidential Information it receives as confidential, safeguard it accordingly and not disclose it to any other person without the prior written permission of the disclosing Party; and
 - 11.1.2 not use or exploit the disclosing Party's Confidential Information in any way except for the purposes anticipated under the Contract.
- 11.2 Notwithstanding clause 11.1, a Party may disclose Confidential Information which it receives from the other Party:
- 11.2.1 where disclosure is required by applicable law or by a court of competent jurisdiction;
 - 11.2.2 to its auditors or for the purposes of regulatory requirements;
 - 11.2.3 on a confidential basis, to its professional advisers;

11.2.4 to the Serious Fraud Office where the Party has reasonable grounds to believe that the other Party is involved in activity that may constitute a criminal offence under the Bribery Act 2010;

11.2.5 where the receiving Party is the Contractor, to the Staff on a need to know basis to enable performance of the Contractor's obligations under the Contract provided that the Contractor shall procure that any Staff to whom it discloses Confidential Information pursuant to this clause - 12546624.47011.2.5 shall observe the Contractor's confidentiality obligations under the Contract; and

11.2.6 where the receiving Party is the Authority:

a) on a confidential basis to the employees, agents, consultants and contractors of the Authority;

b) on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company to which the Authority transfers or proposes to transfer all or any part of its business;

c) to the extent that the Authority (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions; or

11.2.7 in accordance with clause 12.

And for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Authority under this clause 11.

11.3 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of the Contract is not Confidential Information and the Contractor hereby gives its consent for the Authority to publish this Contract in its entirety to the general public (but with any information that is exempt from disclosure in accordance with the FOIA redacted) including any changes to the Contract agreed from time to time. The Authority may consult with the Contractor to inform its decision regarding any redactions but shall have the final decision in its absolute discretion whether any of the content of the Contract is exempt from disclosure in accordance with the provisions of the FOIA.

11.4 The Contractor shall not, and shall take reasonable steps to ensure that the Staff shall not, make any press announcement or publicise the Contract or any part of the Contract in any way, except with the prior written consent of the Authority.

12 Freedom of Information

- 12.1 The Contractor acknowledges that the Authority is subject to the requirements of the FOIA and the Environmental Information Regulations 2004 and shall and procure that any Sub-contractor shall:
 - 12.1.1 provide all necessary assistance and cooperation as reasonably requested by the Authority to enable the Authority to comply with its obligations under the FOIA and the Environmental Information Regulations 2004;
 - 12.1.2 transfer to the Authority all Requests for Information relating to this Contract that it receives as soon as practicable and in any event within 10 Working Days of receipt;
 - 12.1.3 provide the Authority with a copy of all Information belonging to the Authority requested in the Request for Information which is in its possession or control in the form that the Authority requires within 10 Working Days (or such other period as the Authority may reasonably specify) of the Authority's request for such Information; and
 - 12.1.4 not respond directly to a Request for Information unless authorised in writing to do so by the Authority.
- 12.2 The Contractor acknowledges that the Authority may be required under the FOIA and the Environmental Information Regulations 2004 to disclose Information concerning the Contractor or the Services (including commercially sensitive information) without consulting or obtaining consent from the Contractor. In these circumstances the Authority shall, in accordance with any relevant guidance issued under the FOIA, take reasonable steps, where appropriate, to give the Contractor advance notice, or failing that, to draw the disclosure to the Contractor's attention after any such disclosure.
- 12.3 Notwithstanding any other provision in the Contract the Authority shall be responsible for determining in its absolute discretion whether any Information relating to the Contractor or the Services is exempt from disclosure in accordance with the FOIA and/or the Environmental Information Regulations 2004.

13 Protection of Data

13.1 Authority Data

- 13.1.1 The Contractor shall not delete or remove any proprietary notices contained within or relating to the Authority Data.
- 13.1.2 The Contractor shall not store, copy, disclose, or use the Authority Data except as necessary for the performance by the Contractor of its obligations under this Contract or as otherwise expressly authorised in writing by the Authority.

- 13.1.3 To the extent that Authority Data is held and/or Processed by the Contractor, the Contractor shall supply Authority Data to the Authority as requested by the Authority in the format specified in the Specification.
- 13.1.4 The Contractor shall preserve the integrity of Authority Data and prevent the corruption or loss of Authority Data.
- 13.1.5 The Contractor shall perform secure back-ups of all Authority Data and shall ensure that up-to-date back-ups are stored securely off-site. The Contractor shall ensure that such back-ups are made available to the Authority promptly and without undue delay after receipt of a written request from the Authority.
- 13.1.6 The Contractor shall ensure that any system on which the Contractor holds any Authority Data, including back-up data, is a secure system that complies with the Security Policy Framework.
- 13.1.7 If Authority Data is corrupted, lost or sufficiently degraded as a result of the Contractor's Default so as to be unusable, the Authority may:
 - (a) require the Contractor (at the Contractor's expense) to restore or procure the restoration of Authority Data and the Contractor shall do so promptly; and/or
 - (b) itself restore or procure the restoration of Authority Data and shall be repaid by the Contractor any reasonable expenses incurred in doing so.
- 13.1.8 If at any time the Contractor suspects or has reason to believe that Authority Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the Contractor shall notify the Authority immediately and inform the Authority of the remedial action the Contractor proposes to take.

13.2 Personal Data

- 13.2.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Contractor is the Processor
- 13.2.2 The Parties agree that they will comply with the provisions on Processing, Personal Data and Data Subjects in Schedule 4.
- 13.2.3 The Authority requires the Contractor to enter into a data transfer agreement in the form of the Information Commission Office's (ICO) International Data Transfer Agreement with it as set out in Schedule 4 Annex 2.
- 13.2.4 The Contractor is willing and able to enter into the ICO's International Data Transfer Agreement and to comply with its obligations under the provisions of the agreement set out in Schedule 4 Annex 2.
- 13.2.5 The IDTA at Schedule 4 Annex 2 may not be ended at any point during the Term of this Contract.

13.2.6 The Parties shall at all times comply with Data Protection Legislation.

13A Security

- 13A.1 The Authority shall be responsible for maintaining the security of the Authority's premises in accordance with its standard security requirements. The Contractor shall comply with all security requirements of the Authority while on the Authority's premises and shall ensure that all Staff comply with such requirements.
- 13A.2 The Contractor shall ensure that the Security Plan produced by the Contractor complies with Schedule 5 (Security Requirements and Plan).
- 13A.3 The Contractor shall comply, and shall procure compliance of its Staff, with Schedule 5 (Security Requirements and Plan).
- 13A.4 The Authority shall notify the Contractor of any changes or proposed changes to Schedule 5 (Security Requirements and Plan). Any changes shall be agreed in accordance with the procedure in clause 20.3.
- 13A.5 Until and/or unless a change to the Price is agreed by the Authority, the Contractor shall continue to perform the Services in accordance with its existing obligations.
- 13A.5 Subject to the limitations set forth at section 14, the Contractor shall be liable for, and shall indemnify the Authority against all Losses suffered or incurred by the Authority and/or any third party arising from and/or in connection with any Breach of Security or attempted Breach of Security (to the extent that such Losses were not caused by any act or omission by the Authority)

14 Liability and Insurance

14.1 The Contractor shall not be responsible for any injury, loss, damage, cost or expense suffered by the Authority if and to the extent that it is caused by the negligence or wilful misconduct of the Authority or by breach by the Authority of its obligations under the Contract.

14.2 Subject always to clauses 14.3, 14.4 and 14.5:

- 14.2.1 the aggregate liability of the Contractor in respect of all defaults, claims, losses or damages howsoever caused, whether arising from breach of the Contract, the supply or failure to supply of the Services, misrepresentation (whether tortious or statutory), tort (including negligence), breach of statutory duty or otherwise shall in no event exceed a sum equal to 125% of the estimated yearly Price paid or payable to the Contractor under this Contract whichever is higher; and
- 14.2.2 except in the case of claims arising under clauses 9.4 and 18.4 in no event shall the Contractor be liable to the Authority for any:
 - a) loss of profits;

- b) loss of business;
- c) loss of revenue;
- d) loss of or damage to goodwill;
- e) loss of savings (whether anticipated or otherwise); and/or
- f) any indirect, special or consequential loss or damage.

14.3 Nothing in the Contract shall be construed to limit or exclude either Party's liability for:

14.3.1 death or personal injury caused by its negligence or that of its Staff;

14.3.2 fraud or fraudulent misrepresentation by it or that of its Staff; or

14.3.3 any other matter which, by law, may not be excluded or limited.

14.4 The Contractor's liability under the indemnity in clauses 9.4 and 18.4 shall be unlimited.

14.5 The Contractor's liability for all Losses suffered or incurred by the Authority arising from the Contractor's Default resulting in the destruction, corruption, degradation or damage to Authority Data or Personal Data or any copy of such Authority Data or Personal Data shall in no event exceed £250,000.

14.6 The Contractor shall hold:

- a) Employer's liability insurance providing an adequate level of cover in respect of all risks which may be incurred by the Contractor;
- b) Public liability with the minimum cover per claim of one million pounds
£ 1,000,000
- c) Professional indemnity with the minimum cover per claim of one million pounds, £1,000,000

or any sum as required by Law unless otherwise agreed with the Authority in writing. Such insurance shall be maintained for the duration of the Term and for a minimum of six (6) years following the expiration or earlier termination of the Contract.

15 Force Majeure

15.1 Neither Party shall have any liability under or be deemed to be in breach of the Contract for any delays or failures in performance of the Contract which result from circumstances beyond the reasonable control of the Contractor. Each Party shall promptly notify the other Party in writing, using the most expeditious method of delivery, when such circumstances cause a delay or failure in performance, an

estimate of the length of time delay or failure shall continue and when such circumstances cease to cause delay or failure in performance. If such circumstances continue for a continuous period of more than 30 days, either Party may terminate the Contract by written notice to the other Party

- 15.2 Any failure by the Contractor in performing its obligations under the Contract which results from any failure or delay by an agent, Sub-contractor or Contractor shall be regarded as due to Force Majeure only if that agent, Sub-contractor or Contractor is itself impeded by Force Majeure from complying with an obligation to the Contractor.

16 Termination

- 16.1 The Authority may terminate the Contract at any time by notice in writing to the Contractor to take effect on any date falling at least 1 month (or, if the Contract is less than 3 months in duration, at least 10 Working Days) later than the date of service of the relevant notice.
- 16.2 Without prejudice to any other right or remedy it might have, the Authority may terminate the Contract by written notice to the Contractor with immediate effect if the Contractor:
- 16.2.1 (without prejudice to clause 16.2.5), is in material breach of any obligation under the Contract which is not capable of remedy;
 - 16.2.2 repeatedly breaches any of the terms and conditions of the Contract in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms and conditions of the Contract;
 - 16.2.3 is in material breach of any obligation which is capable of remedy, and that breach is not remedied within 30 days of the Contractor receiving notice specifying the breach and requiring it to be remedied;
 - 16.2.4 undergoes a change of control within the meaning of section 1124 of the Corporation Tax Act 2010;
 - 16.2.5 breaches any of the provisions of clauses 7.2, 11, 12, 13, 17, 18.4 and 20.11; or
 - 16.2.6 becomes insolvent, or if an order is made or a resolution is passed for the winding up of the Contractor (other than voluntarily for the purpose of solvent amalgamation or reconstruction), or if an administrator or administrative receiver is appointed in respect of the whole or any part of the Contractor's assets or business, or if the Contractor makes any composition with its creditors or takes or suffers any similar or analogous action (to any of the actions detailed in this clause 16.2.6) in consequence of debt in any jurisdiction.

- 16.3 The Contractor shall notify the Authority as soon as practicable of any change of control as referred to in clause 16.2.4 or any potential such change of control.
- 16.4 The Contractor may terminate the Contract by written notice to the Authority if the Authority has not paid any undisputed amounts within 90 days of them falling due.
- 16.5 If the Authority terminates the Contract under this clause, the Authority shall make no further payments to the Contractor except for Services supplied by the Contractor prior to termination and in accordance with the Contract but where the payment has yet to be made by the Authority.
- 16.6 Termination or expiry of the Contract shall be without prejudice to the rights of either Party accrued prior to termination or expiry and shall not affect the continuing rights of the Parties under this clause and clauses 2, 3.4, 6.1, 6.2, 6.6, 6.7, 7, 9, 10.2, 11, 12, 13, 13A, 0, 16.7, 17.4, 18.4, 19 and 20.8 or any other provision of the Contract that either expressly or by implication has effect after termination.
- 16.7 Upon termination or expiry of the Contract, the Contractor shall:
- 16.7.1 give all reasonable assistance to the Authority and any incoming Contractor of the Services to the extent necessary to effect an orderly assumption by a Replacement Contractor in accordance with the procedure set out in Schedule 8 – Exit Management Strategy; and
 - 16.7.2 return all requested documents, information and data to the Authority as soon as reasonably practicable.

17 Compliance

- 17.1 The Contractor shall promptly notify the Authority of any health and safety hazards which may arise in connection with the performance of its obligations under the Contract. The Authority shall promptly notify the Contractor of any health and safety hazards which may exist or arise at the Authority's premises and which may affect the Contractor in the performance of its obligations under the Contract.
- 17.2 The Contractor shall:
- 17.2.1 comply with all the Authority's health and safety measures while on the Authority's premises; and
 - 17.2.2 notify the Authority immediately of any incident occurring in the performance of its obligations under the Contract on the Authority's premises where that incident causes any personal injury or damage to property which could give rise to personal injury.
- 17.3 The Contractor shall:

- 17.3.1 perform its obligations under the Contract in accordance with all applicable equality Law and the Authority's equality and diversity policy as provided to the Contractor from time to time; and
- 17.3.2 take all reasonable steps to secure the observance of clause 17.3.1 by all Staff.
- 17.4 The Contractor shall supply the Services in accordance with the Authority's environmental policy as provided to the Contractor from time to time.
- 17.5 The Contractor shall comply with, and shall ensure that its Staff shall comply with, the provisions of:
 - 17.5.1 the Official Secrets Acts 1911 to 1989; and
 - 17.5.2 section 182 of the Finance Act 1989.

18 Prevention of Fraud, Corruption and Bribery

- 18.1 The Contractor represents and warrants that neither it, nor to the best of its knowledge any Staff, have at any time prior to the Commencement Date:
 - 18.1.1 Committed a Prohibited Act or been formally notified that it is subject to an investigation or prosecution which relates to an alleged Prohibited Act and/or
 - 18.1.2 Been listed by any government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in government procurement programmes or contracts on the grounds of a Prohibited Act.
- 18.2 The Contractor shall not during the Term:
 - 18.2.1 commit a Prohibited Act; and/or
 - 18.2.2 do or suffer anything to be done which would cause the Authority or any of its employees, consultants, contractors, Sub-contractors or agents to contravene any of the Relevant Requirements or otherwise incur any liability in relation to the Relevant Requirements.
- 18.3 The Contractor shall, during the Term establish, maintain and enforce, and require that its Sub-Contractors establish, maintain and enforce, policies and procedures which are adequate to ensure compliance with the Relevant Requirements and prevent the occurrence of a Prohibited Act; and shall notify the Authority immediately if it has reason to suspect that any breach of clauses 18.1 and/or 18.2 has occurred or is occurring or is likely to occur.
- 18.4 If the Contractor or the Staff engages in conduct prohibited by clause 18.1 or commits fraud in relation to the Contract or any other contract with the Crown (including the Authority) the Authority may:

- 18.4.1 terminate the Contract and recover from the Contractor the amount of any loss suffered by the Authority resulting from the termination, including the cost reasonably incurred by the Authority of making other arrangements for the supply of the Services and any additional expenditure incurred by the Authority throughout the remainder of the Contract; or
- 18.4.2 recover in full from the Contractor any other loss sustained by the Authority in consequence of any breach of this clause.

19 Dispute Resolution

- 19.1 The Parties shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the Contract within 20 Working Days of either Party notifying the other of the dispute and such efforts shall involve the escalation of the dispute to an appropriately senior representative of each Party.
- 19.2 If the dispute cannot be resolved by the Parties within one month of being escalated as referred to in clause 19.1, the dispute may by agreement between the Parties be referred to a neutral adviser or mediator (the “Mediator”) chosen by agreement between the Parties. All negotiations connected with the dispute shall be conducted in confidence and without prejudice to the rights of the Parties in any further proceedings.
- 19.3 If the Parties fail to appoint a Mediator within one month 20 Working Days of the agreement to refer to a Mediator, either Party shall apply to the Centre for Effective Dispute Resolution to appoint a Mediator.
- 19.4 If the Parties fail to enter into a written agreement resolving the dispute within one month of the Mediator being appointed, or such longer period as may be agreed by the Parties, either Party may refer the dispute to Court.
- 19.5 The commencement of mediation shall not prevent the parties commencing or continuing court or arbitration proceedings in relation to the dispute.

20 General

- 20.1 Each of the Parties represents and warrants to the other that it has full capacity and authority, and all necessary consents, licences and permissions to enter into and perform its obligations under the Contract, and that the Contract is executed by its duly authorised representative.
- 20.2 A person who is not a party to the Contract shall have no right to enforce any of its provisions which, expressly or by implication, confer a benefit on him, without the prior written agreement of the Parties. This clause does not affect any right or remedy of any person which exists or is available apart from the Contracts (Rights of Third Parties) Act 1999 and does not apply to the Crown.

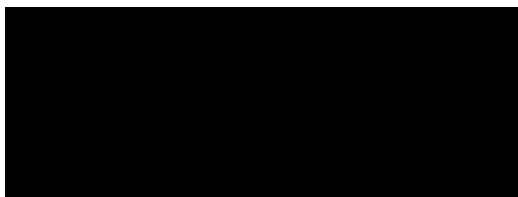
- 20.3 Subject to Clause 3.4, the Contract cannot be varied except in writing signed by a duly authorised representative of both the Parties.
- 20.4 In the event that the Contractor is unable to accept the Variation to the Specification or where the Parties are unable to agree a change to the Contract Price, the Authority may:
- 20.4.1 allow the Contractor to fulfil its obligations under the Contract without the Variation to the Specification;
 - 20.4.2 terminate the Contract with immediate effect, except where the Contractor has already provided all or part of the Services or where the Contractor can show evidence of substantial work being carried out to fulfil the requirement of the Specification, and in such case the Parties shall attempt to agree upon a resolution to the matter. Where a resolution cannot be reached, the matter shall be dealt with under the Dispute Resolution procedure detailed at clause 19.
- 20.5 The Contract contains the whole agreement between the Parties and supersedes and replaces any prior written or oral agreements, representations or understandings between them. The Parties confirm that they have not entered into the Contract on the basis of any representation that is not expressly incorporated into the Contract. Nothing in this clause shall exclude liability for fraud or fraudulent misrepresentation.
- 20.6 Any waiver or relaxation either partly, or wholly of any of the terms and conditions of the Contract shall be valid only if it is communicated to the other Party in writing and expressly stated to be a waiver. A waiver of any right or remedy arising from a breach of contract shall not constitute a waiver of any right or remedy arising from any other breach of the Contract.
- 20.7 The Contract shall not constitute or imply any partnership, joint venture, agency, fiduciary relationship or other relationship between the Parties other than the contractual relationship expressly provided for in the Contract. Neither Party shall have, nor represent that it has, any authority to make any commitments on the other Party's behalf.
- 20.8 Except as otherwise expressly provided by the Contract, all remedies available to either Party for breach of the Contract (whether under the Contract, statute or common law) are cumulative and may be exercised concurrently or separately, and the exercise of one remedy shall not be deemed an election of such remedy to the exclusion of other remedies.
- 20.9 If any provision of the Contract is prohibited by law or judged by a court to be unlawful, void or unenforceable, the provision shall, to the extent required, be severed from the Contract and rendered ineffective as far as possible without modifying the remaining provisions of the Contract, and shall not in any way affect any other circumstances of or the validity or enforcement of the Contract.

- 20.10 The Contractor shall take appropriate steps to ensure that neither the Contractor nor any Staff is placed in a position where, in the reasonable opinion of the Authority, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Contractor and the duties owed to the Authority under the provisions of the Contract. The Contractor will disclose to the Authority full particulars of any such conflict of interest which may arise.
- 20.11 The Authority reserves the right to terminate the Contract immediately by notice in writing and/or to take such other steps it deems necessary where, in the reasonable opinion of the Authority, there is or may be an actual conflict, or potential conflict between the pecuniary or personal interest of the Contractor and the duties owed to the Authority pursuant to this clause shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereafter accrue to the Authority.
- 20.12 The Contract constitutes the entire agreement between the Parties in respect of the matters dealt with therein. The Contract supersedes all prior negotiations between the Parties and all representations and undertakings made by one Party to the other, whether written or oral, except that this clause shall not exclude liability in respect of any Fraud or fraudulent misrepresentation.

21 Notices

- 21.1 Except as otherwise expressly provided in the Contract, no notice or other communication from one Party to the other shall have any validity under the Contract unless made in writing by or on behalf of the Party concerned.
- 21.2 Any notice or other communication which is to be given by either Party to the other shall be given by letter (sent by hand, first class post, recorded delivery or special delivery), or by facsimile transmission or electronic mail (confirmed in either case by letter), Such letters shall be addressed to the other Party in the manner referred to in clause 21.3. Provided the relevant communication is not returned as undelivered, the notice or communication shall be deemed to have been given 2 Working Days after the day on which the letter was posted, or 4 hours, in the case of electronic mail or facsimile transmission or sooner where the other Party acknowledges receipt of such letters, facsimile transmission or item of electronic mail.
- 21.3 For the purposes of clause 21.2, the address of each Party shall be:
- 21.3.1 For the Authority:

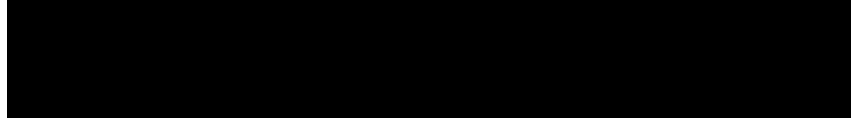
Address: Citygate Gallowgate Newcastle upon Tyne NE1 4PA



21.3.2 For the Contractor:

Address: the Connection, 198 High Holborn, London, WC1V 7BD, UNITED KINGDOM

For the attention of General Counsel



21.4 Either Party may change its address for service by serving a notice in accordance with this clause.

21.5 Notices under clauses 0 (Force Majeure) and 16 (Termination) may be served by email only if the original notice is then sent to the recipient by personal delivery or recorded delivery in the manner set out in clause 21.1.

22 Governing Law and Jurisdiction

22.1 The validity, construction and performance of the Contract, and all contractual and non-contractual matters arising out of it, shall be governed by English law and shall be subject to the exclusive jurisdiction of the English courts to which the Parties submit.

23 TUPE not used

IN WITNESS of which this Contract has been duly executed by the parties.

SIGNED for and on behalf of **CARE QUALITY COMMISSION**

Authorised Signatory:

SIGNED for and on behalf of **Development Dimensions International (UK) Ltd**

DDI Legal Approval Initials 2:

Authorised Signatory 1:

Authorised Signatory 2:

SCHEDULE 1 –SPECIFICATION

The Requirement

CQC wish to deliver its successful Manager programme and would want to continue to access learning materials on a pay per delegate per course basis. Learning events can only be delivered by accredited facilitators who have undergone preparation.

To deliver goals set out in the People Plan CQC requires ongoing access to this learning resource for a further 12 months.

CQC will require access for additional facilitation training for Academy colleagues as new colleagues join the team and others move into different roles.

This will be call off arrangement and as such there are no volumes or numbers guaranteed. CQC would require purchase of materials for the following learning modules and additional titles if required:

- Communication: Connection Through Conversations
- Creating an Inclusive Environment
- Embracing Change
- Goal Setting and Reviewing Results
- Addressing Poor Performance
- Leading Virtually

CQC will require the ability to purchase further facilitator packs for each courses any new facilitators are trained on.

CQC require the ability to purchase of places (online or in-person) on open facilitator training courses OR the requirement to have a facilitator training course run solely for CQC Academy colleagues (online or in-person) if there is sufficient demand for such a course.

System

All files must be SCORM 1.2, SCORM 2004, or AICC compliant and in zip files.

Note: Currently, SCORM 2004 3rd edition is implemented. Backward compatibility is generally expected, and thus courses published in 2nd edition are likely to work properly, but it is advised that courses are created using SCORM 2004 3rd edition.

The majority of CQC staff are home-workers and as such will usually access our LMS on a remote connection. A great number of our home-workers reside in areas with below average broadband speeds/bandwidths – some as low as 0.2mbps.

- Our workforce accesses our LMS on a variety of devices and browsers – so E-Learning or materials should be designed to function on all modern browsers (Internet Explorer, Safari, Chrome & Firefox) – this includes designing and publishing SCORM files with HTML5 and SWF compatibility.

ACCESSIBILITY STANDARDS

The supplier commits to evaluate specific accessibility needs of each disabled CQC Participant on a case-by-case basis in partnership with CQC. The products satisfy the need, established under the Americans With Disabilities Act, for providing equivalent alternatives for accessibility by disabled individuals. The products satisfy most standards contained in the Web Content Accessibility Guidelines as well as Section 508 of the Rehabilitation Act (1973). The supplier is committed to supporting all Participants with disabilities, the high-fidelity nature of many of the products' designs limits full compliance under Section 508 (e.g. high-contrast settings, ...)

SCHEDULE 2 – PRICE

Volumes are only indicative; the Authority does not guarantee any volumes. Modules will be ordered by the Authority as and when required. The maximum total value of the contract will not exceed the Price Cap of £60,000 inc VAT. However, no Module is guaranteed to be ordered by the Authority.

[illegible]

INVOICING INSTRUCTIONS

Payment

All invoices must be posted to the address below:



Or emailed the email address is: sbs.invoicing@nhs.net.

The criteria which your invoices must meet are:

Invoices must comply with our [Good Invoicing Practice](#)

- This ensures all correct data is within the Invoice in a consistent way

Only PDF email attachments can be accepted

- Other file types and nested emails cannot be accepted and will be deleted.

One invoice per PDF

- Backing documents must be included in the same PDF as the relevant invoice
- Emails with multiple PDFs are acceptable. For example
- 10 PDFs with 1 invoice per PDF **will** be accepted
- 1 PDF with 10 invoices within will **not** be accepted

Emails must not exceed 10Mb

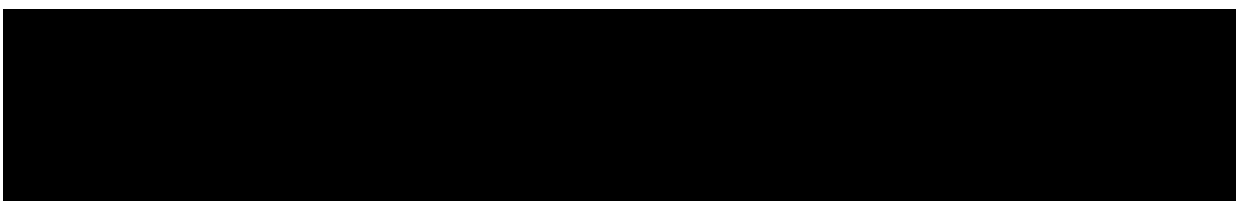
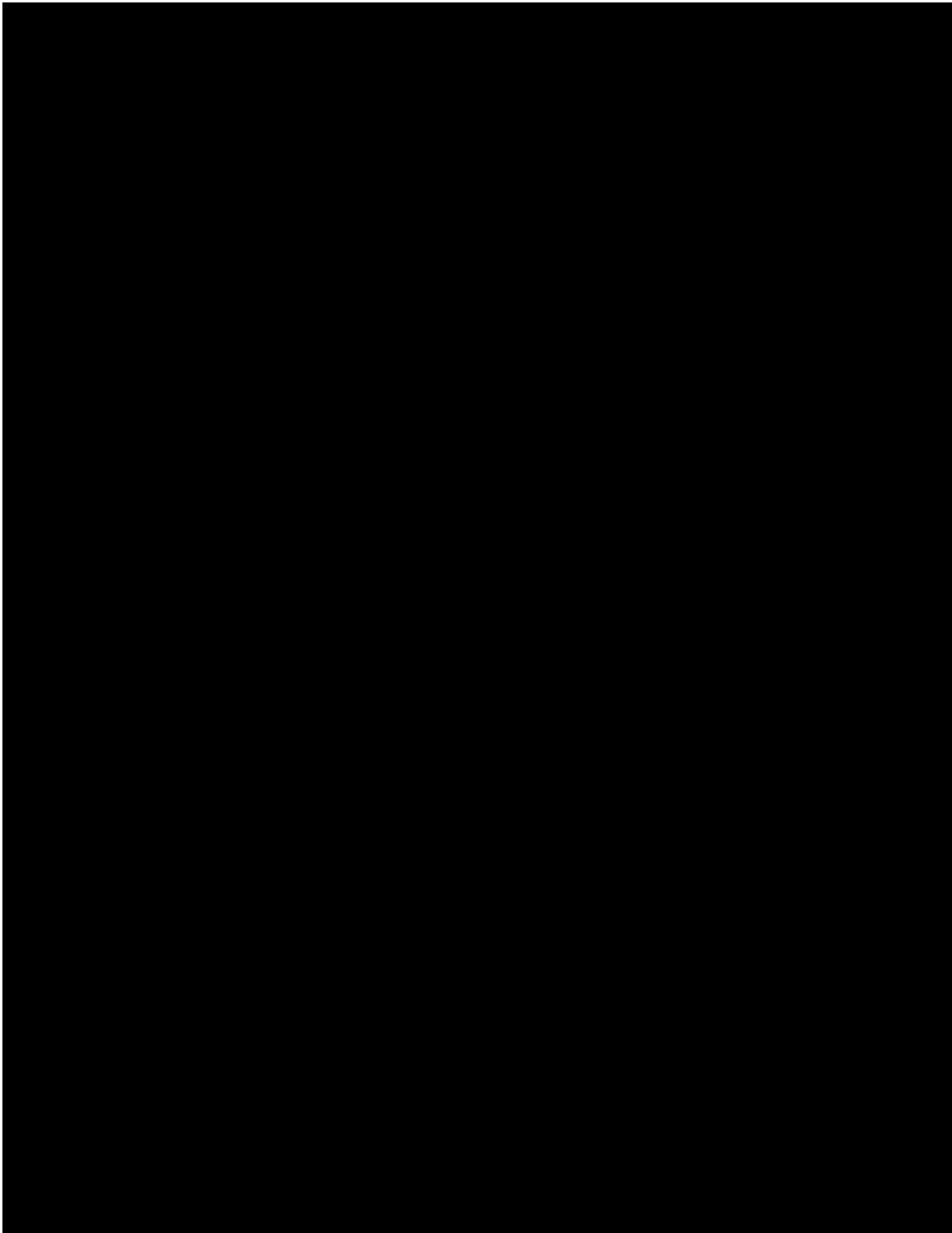
For information on how to do this please see our guidance online here:

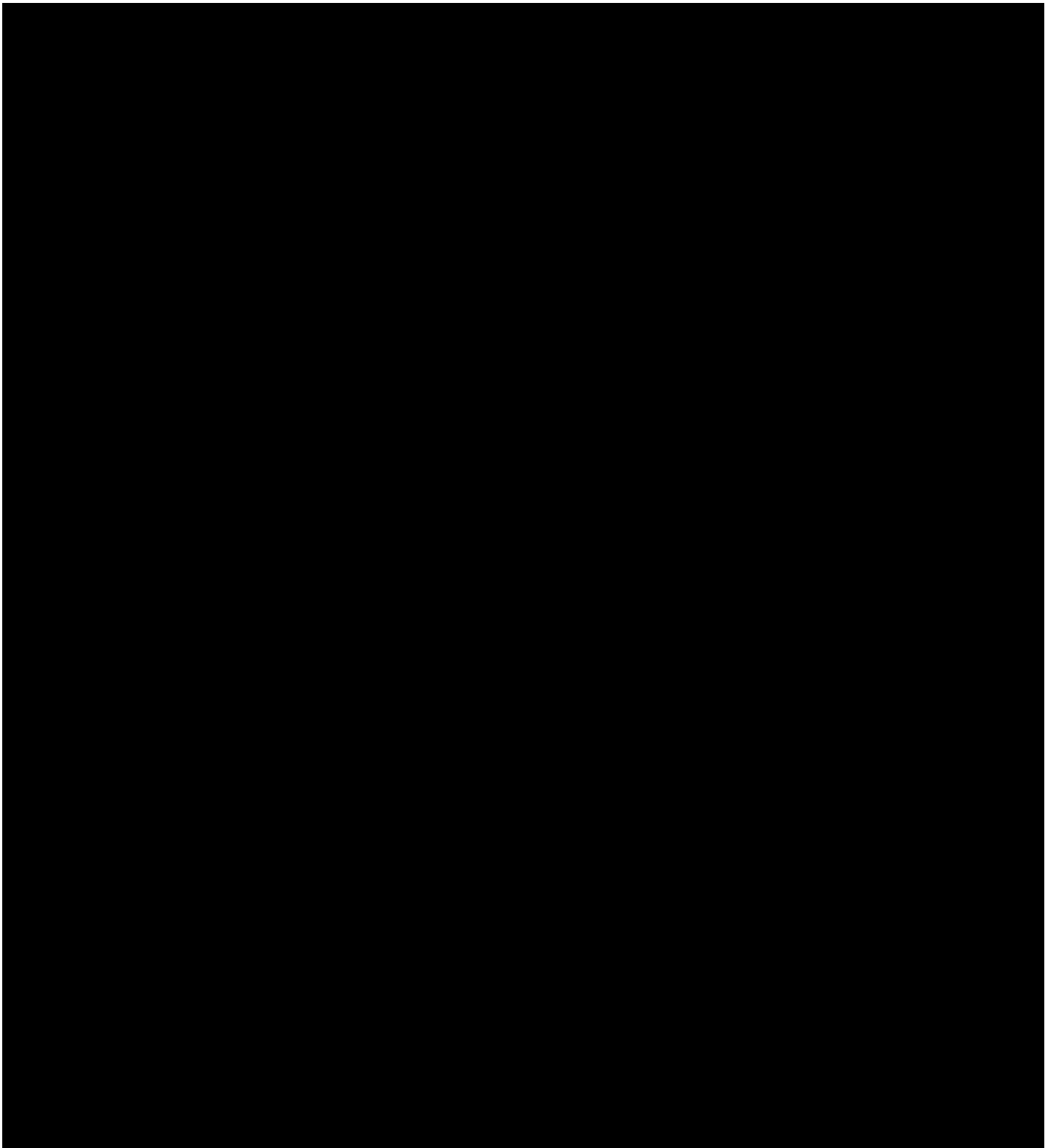
<https://www.sbs.nhs.uk/faq-fasub-inv-how-to-nhs-sbs>

Purchase Order

A Purchase Order number will be provided which must be quoted on each invoice, the supplier shall invoice CQC monthly in arrears – for modules accessed in the previous month.

SCHEDULE 3 – CONTRACTOR’S RESPONSE





SCHEDULE 4 – PROCESSING, PERSONAL DATA AND DATA SUBJECTS

- 1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Contractor is the Processor. The only processing that the Processor is authorised to do is listed in Annex 1 to this Schedule 4 by the Controller and may not be determined by the Processor. The term “processing” and any associated terms are to be read in accordance with Article 4 of the UK GDPR.
- 2 The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.
- 3 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:
 - (a) a systematic description of the envisaged processing operations and the purpose of the processing;
 - (b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;
 - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
 - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
- 4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Contract:
 - (a) process that Personal Data only in accordance with Annex 1 to this Schedule 4, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;
 - (b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject. In the event of the Controller reasonably rejecting Protective Measures put in place by the Processor, the Processor must propose alternative Protective Measures to the reasonable satisfaction of the Controller. Failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures. Protective Measures must take account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Data Loss Event;
 - (iii) state of technological development; and

- (iv) cost of implementing any measures;
- (c) ensure that:
 - (i) the Processor Personnel do not process Personal Data except in accordance with this Contract (and in particular Annex 1 to this Schedule 4);
 - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (A) are aware of and comply with the Processor's duties under this clause;
 - (B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
 - (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Contract; and
 - (D) have undergone adequate training in the use, care, protection and handling of Personal Data; and
- (d) not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
 - (i) the destination country has been recognised as adequate by the UK government in accordance with Article 45 UK GDPR or section 74 of the DPA 2018;
 - (ii) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 DPA 2018) as determined by the Controller;
 - (iii) the Data Subject has enforceable rights and effective legal remedies;
 - (iv) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
- (v) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;
- (e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

5 Subject to paragraph 6, the Processor shall notify the Controller without undue delay if it:

- (a) receives a Data Subject Access Request (or purported Data Subject Access Request);
- (b) receives a request to rectify, block or erase any Personal Data;

- (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;
 - (e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
 - (f) becomes aware of a Data Loss Event.
- 6 The Processor's obligation to notify under paragraph 5 shall include the provision of further information to the Controller, as details become available.
- 7 Taking into account the nature of the processing, the Processor shall provide the Controller with reasonable assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 5 (and insofar as possible within the timescales reasonably required by the Controller) including but not limited to promptly providing:
 - (a) the Controller with full details and copies of the complaint, communication or request;
 - (b) such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;
 - (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
 - (d) assistance as requested by the Controller following any Data Loss Event;
 - (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.
- 8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this paragraph. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
 - (a) the Controller determines that the processing is not occasional;
 - (b) the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
 - (c) the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.
- 9 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

- 10 Each Party shall designate its own data protection officer if required by the Data Protection Legislation.
- 11 Before allowing any Sub-processor to process any Personal Data related to this Contract, the Processor must:
 - (a) notify the Controller in writing of the intended Sub-processor and processing;
 - (b) obtain the written consent of the Controller;
 - (c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this Schedule 4 such similar terms apply in a no less restrictive manner to the Sub-processor; and
 - (d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

The forgoing notwithstanding, Authority acknowledges that Contractor may utilize one or more subprocessor in the ordinary course and scope of its business operations for ancillary services. Authority provides general authorization for use of the subprocessors on the list at the link provided: <https://corp.ddiworld.com/thirdpartyproviders> . Contractor will be responsible for the actions of such in their performance of Services provided hereunder and shall inform Authority of any intended changes concerning the addition or replacement of other subprocessors

- 12 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.
- 13 The Controller may, at any time on not less than 30 Working Days' notice, revise this paragraph by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Contract).
- 14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.
- 15 Subject to clause 14.5, the Processor shall indemnify the Controller on a continuing basis against any and all Losses incurred by the Controller arising from the Processor's Default under this Schedule 4 and/or any failure by the Processor or any Sub-processor to comply with their respective obligations under Data Protection Legislation.
- 16 Nothing in this Schedule 4 shall be construed as requiring the Processor or any relevant Sub-processor to be in breach of any Data Protection Legislation.
17. The Controller acknowledges that all of the Processor's data servers are in the United States. The Controller authorizes the Processor to transfer and process all Personal Data obtained under this Contract in the United States on the condition that the Processor complies with the provisions set out within the International Data Transfer Agreement (IDTA) set out in Annex 2 of this Schedule 4.
18. The processor shall comply with the provisions of the International Data Transfer Agreement (IDTA) as set out in Annex 2 of this Schedule 4.

ANNEX 1 – Data Processing Schedule, Personal Data and Data Subjects Schedule

1. The contact details of the Controller's Data Protection Officer are: [REDACTED] Care Quality Commission, Citygate, Gallowgate, Newcastle Upon Tyne, NE1 4PA, United Kingdom.
2. The contact details of the Processor's Data Protection Officer are: DataProtectionOfficer@ddiworld.com
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
4. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Contractor is the Processor in accordance with paragraph 1 of this Schedule 4.
Subject matter of the processing	This is to enable CQC to have access to learner materials for line managers who wish to undertake online learning modules offered by DDI
Duration of the processing	The duration of the contract which is from 1 st September 2023 to 31 st August 2024
Nature and purposes of the processing	The Academy have accredited DDI facilitators within the training team who deliver DDI modules to the wider organisation as part of the People Plan. CQC purchases learner materials for anyone who wants to do any of these learning modules. CQC need to process information about the names and numbers of learners who we purchase materials for to enable DDI to send out the course material to individuals.
Type of personal data	Name and email addresses
Categories of Data Subject	CQC Employees – Line Managers

International transfers and legal gateway	Data is stored In the US, and may be accessed from US, UK, India and AU. Transfers are supported by EU SCCs and UK IDTA, annexed to this contract.
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	DDI will retain your information for as long as your account is active or as needed to provide you services including statistical normalization, for a maximum of 5 years post user inactivity. We will retain and use your information in anonymized format for research purposes and as necessary, to comply with our legal obligations, resolve disputes, and enforce our agreements.

ANNEX 2 International Data Transfer Agreement

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Agreement

VERSION A1.0, in force 21 March 2022









This IDTA has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

For the purpose of this IDTA, the Care Quality Commission shall be the Exporter and Development Dimensions International (UK) shall be the Importer.

Part 1: Tables

Table 1: Parties and signatures

Start date	1 st September 2023	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: Care Quality Commission Trading name (if different): Main address (if a company registered address): Citygate Gallowgate Newcastle upon Tyne NE1 4PA	Full legal name: Development Dimensions International (UK)Ltd, Trading name (if different): Main address (if a company registered address): The Connection, 198 High Holborn, London, WC1V 7BD.

	Official registration number (if any) (company number or similar identifier):	Official registration number (if any) (company number or similar identifier): Company Number 01683848
Key Contact		    
Importer Data Subject Contact		Job Title: DPO  
Signatures confirming each Party agrees to be bound by this IDTA	Signed for and on behalf of the Exporter set out above Exporter Signature and Date:	

	Signed for and on behalf of the Importer set out above Importer Signature and Date:
	DDI Legal Approval Initials 1:

Table 2: Transfer Details

Table 2: Transfer Details	
UK country's law that governs the IDTA:	<input checked="" type="checkbox"/> England and Wales Northern Ireland Scotland
Primary place for legal claims to be made by the Parties	<input checked="" type="checkbox"/> England and Wales <input type="checkbox"/> Northern Ireland <input type="checkbox"/> Scotland
The status of the Exporter	In relation to the Processing of the Transferred Data: <input checked="" type="checkbox"/> Exporter is a Controller

	<input type="checkbox"/> Exporter is a Processor or Sub-Processor
The status of the Importer	<p>In relation to the Processing of the Transferred Data:</p> <input type="checkbox"/> Importer is a Controller <input checked="" type="checkbox"/> Importer is the Exporter's Processor or Sub-Processor <input type="checkbox"/> Importer is not the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)
Whether UK GDPR applies to the Importer	<input checked="" type="checkbox"/> UK GDPR applies to the Importer's Processing of the Transferred Data <input type="checkbox"/> UK GDPR does not apply to the Importer's Processing of the Transferred Data
Linked Agreement	<p>If the Importer is the Exporter's Processor or Sub-Processor – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data:</p> <p>Name of agreement: Contract for the provision of a call off facility of training modules for First-Level and Mid-Level Leadership</p> <p>Date of agreement: 1st September 2023</p> <p>Parties to the agreement: the Care Quality Commission and Development Dimensions International (UK) only</p> <p>Reference (if any): CQC RCCO 083</p> <p>Other agreements – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement:</p> <p>Name of agreement:</p> <p>Date of agreement:</p> <p>Parties to the agreement:</p> <p>Reference (if any):</p> <p>If the Exporter is a Processor or Sub-Processor – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data:</p>

	Name of agreement: Date of agreement: Parties to the agreement: Reference (if any):
Term	The Importer may Process the Transferred Data for the following time period: <input checked="" type="checkbox"/> the period for which the Linked Agreement is in force <input type="checkbox"/> time period: <input type="checkbox"/> (only if the Importer is a Controller or not the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose.
Ending the IDTA before the end of the Term	<input checked="" type="checkbox"/> the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing. <input type="checkbox"/> the Parties can end the IDTA before the end of the Term by serving: <input type="text"/> months' written notice, as set out in Section 29 (How to end this IDTA without there being a breach).
Ending the IDTA when the Approved IDTA changes	Which Parties may end the IDTA as set out in Section 29.2: <input checked="" type="checkbox"/> Importer <input checked="" type="checkbox"/> Exporter <input type="checkbox"/> neither Party
Can the Importer make further transfers of the Transferred Data?	<input checked="" type="checkbox"/> The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data). <input type="checkbox"/> The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).

Specific restrictions when the Importer may transfer on the Transferred Data	<p>The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1:</p> <p><input type="checkbox"/> if the Exporter tells it in writing that it may do so.</p> <p><input type="checkbox"/> to:</p> <p><input checked="" type="checkbox"/> to the authorised receivers (or the categories of authorised receivers) set out in: the Linked Agreement</p> <p><input type="checkbox"/> there are no specific restrictions.</p>
Review Dates	<p><input checked="" type="checkbox"/> No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data</p> <p>First review date:</p> <p>The Parties must review the Security Requirements at least once:</p> <p><input type="checkbox"/> each month(s)</p> <p><input type="checkbox"/> each quarter</p> <p><input type="checkbox"/> each 6 months</p> <p><input type="checkbox"/> each year</p> <p><input type="checkbox"/> each year(s)</p> <p><input type="checkbox"/> each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment</p>

Table 3: Transferred Data

Transferred Data	<p>The personal data to be sent to the Importer under this IDTA consists of:</p> <p><input checked="" type="checkbox"/> The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to.</p> <p><input type="checkbox"/> The categories of Transferred Data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.</p>
Special Categories of Personal Data and criminal	<p>The Transferred Data includes data relating to:</p> <p><input type="checkbox"/> racial or ethnic origin</p> <p><input type="checkbox"/> political opinions</p>

convictions and offences	<div data-bbox="469 174 1422 703"> <input type="checkbox"/> religious or philosophical beliefs <input type="checkbox"/> trade union membership <input type="checkbox"/> genetic data <input type="checkbox"/> biometric data for the purpose of uniquely identifying a natural person <input type="checkbox"/> physical or mental health <input type="checkbox"/> sex life or sexual orientation <input type="checkbox"/> criminal convictions and offences <input checked="" type="checkbox"/> none of the above <input type="checkbox"/> set out in: </div> <div data-bbox="469 770 1422 1122"> <p>And:</p> <input checked="" type="checkbox"/> The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The categories of special category and criminal records data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3. </div>
Relevant Data Subjects	<div data-bbox="469 1189 1422 1541"> <p>The Data Subjects of the Transferred Data are:</p> <input checked="" type="checkbox"/> The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The categories of Data Subjects will not update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3. </div>
Purpose	<div data-bbox="469 1612 1422 1883"> <input type="checkbox"/> The Importer may Process the Transferred Data for the following purposes: See contract <input type="checkbox"/> The Importer may Process the Transferred Data for the purposes set out in: <p>In both cases, any other purposes which are compatible with the purposes set out above.</p> </div>

	<input checked="" type="checkbox"/> The purposes will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under 5.3.
--	--

Table 4: Security Requirements

Security of Transmission	As per the provisions set out in Schedule 5 of the Linked Agreement
Security of Storage	As per the provisions set out in Schedule 5 of the Linked Agreement
Security of Processing	As per the provisions set out in Schedule 5 of the Linked Agreement
Organisational security measures	As per the provisions set out in Schedule 5 of the Linked Agreement
Technical security minimum requirements	As per the provisions set out in Schedule 5 of the Linked Agreement
Updates to the Security Requirements	<input checked="" type="checkbox"/> The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Part 2: Extra Protection Clauses

Extra Protection Clauses:	Not Used
----------------------------------	----------

(i) Extra technical security protections	
(ii) Extra organisational protections	
(iii) Extra contractual protections	

Part 3: Commercial Clauses

Commercial Clauses	Not Used
---------------------------	----------

Part 4: Mandatory Clauses

Information that helps you to understand this IDTA

1. This IDTA and Linked Agreements

- 1.1 Each Party agrees to be bound by the terms and conditions set out in the IDTA, in exchange for the other Party also agreeing to be bound by the IDTA.
- 1.2 This IDTA is made up of:
 - 1.2.1 Part one: Tables;
 - 1.2.2 Part two: Extra Protection Clauses;
 - 1.2.3 Part three: Commercial Clauses; and
 - 1.2.4 Part four: Mandatory Clauses.
- 1.3 The IDTA starts on the Start Date and ends as set out in Sections 29 or 30.
- 1.4 If the Importer is a Processor or Sub-Processor instructed by the Exporter: the Exporter must ensure that, on or before the Start Date and during the Term, there is a Linked Agreement which is enforceable between the Parties and which

complies with Article 28 UK GDPR (and which they will ensure continues to comply with Article 28 UK GDPR).

- 1.5 References to the Linked Agreement or to the Commercial Clauses are to that Linked Agreement or to those Commercial Clauses only in so far as they are consistent with the Mandatory Clauses.

2. Legal Meaning of Words

- 2.1 If a word starts with a capital letter it has the specific meaning set out in the Legal Glossary in Section 36.
- 2.2 To make it easier to read and understand, this IDTA contains headings and guidance notes. Those are not part of the binding contract which forms the IDTA.

3. You have provided all the information required

- 3.1 The Parties must ensure that the information contained in Part one: Tables is correct and complete at the Start Date and during the Term.
- 3.2 In Table 2: Transfer Details, if the selection that the Parties are Controllers, Processors or Sub-Processors is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws) then:
 - 3.2.1 the terms and conditions of the Approved IDTA which apply to the correct option which was not selected will apply; and
 - 3.2.2 the Parties and any Relevant Data Subjects are entitled to enforce the terms and conditions of the Approved IDTA which apply to that correct option.
- 3.3 In Table 2: Transfer Details, if the selection that the UK GDPR applies is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws), then the terms and conditions of the IDTA will still apply to the greatest extent possible.

4. How to sign the IDTA

- 4.1 The Parties may choose to each sign (or execute):
 - 4.1.1 the same copy of this IDTA;
 - 4.1.2 two copies of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement;
 - 4.1.3 a separate, identical copy of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement,

unless signing (or executing) in this way would mean that the IDTA would not be binding on the Parties under Local Laws.

5. Changing this IDTA

- 5.1 Each Party must not change the Mandatory Clauses as set out in the Approved IDTA, except only:
- 5.1.1 to ensure correct cross-referencing: cross-references to Part one: Tables (or any Table), Part two: Extra Protections, and/or Part three: Commercial Clauses can be changed where the Parties have set out the information in a different format, so that the cross-reference is to the correct location of the same information, or where clauses have been removed as they do not apply, as set out below;
 - 5.1.2 to remove those Sections which are expressly stated not to apply to the selections made by the Parties in Table 2: Transfer Details, that the Parties are Controllers, Processors or Sub-Processors and/or that the Importer is subject to, or not subject to, the UK GDPR. The Exporter and Importer understand and acknowledge that any removed Sections may still apply and form a part of this IDTA if they have been removed incorrectly, including because the wrong selection is made in Table 2: Transfer Details;
 - 5.1.3 so the IDTA operates as a multi-party agreement if there are more than two Parties to the IDTA. This may include nominating a lead Party or lead Parties which can make decisions on behalf of some or all of the other Parties which relate to this IDTA (including reviewing Table 4: Security Requirements and Part two: Extra Protection Clauses, and making updates to Part one: Tables (or any Table), Part two: Extra Protection Clauses, and/or Part three: Commercial Clauses); and/or
 - 5.1.4 to update the IDTA to set out in writing any changes made to the Approved IDTA under Section 5.4, if the Parties want to. The changes will apply automatically without updating them as described in Section 5.4;
- provided that the changes do not reduce the Appropriate Safeguards.
- 5.2 If the Parties wish to change the format of the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of the Approved IDTA, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- 5.3 If the Parties wish to change the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of this IDTA (or the equivalent information), they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

5.4 From time to time, the ICO may publish a revised Approved IDTA which:

5.4.1 makes reasonable and proportionate changes to the Approved IDTA, including correcting errors in the Approved IDTA; and/or

5.4.2 reflects changes to UK Data Protection Laws.

The revised Approved IDTA will specify the start date from which the changes to the Approved IDTA are effective and whether an additional Review Date is required as a result of the changes. This IDTA is automatically amended as set out in the revised Approved IDTA from the start date specified.

6. Understanding this IDTA

6.1 This IDTA must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

6.2 If there is any inconsistency or conflict between UK Data Protection Laws and this IDTA, the UK Data Protection Laws apply.

6.3 If the meaning of the IDTA is unclear or there is more than one meaning, the meaning which most closely aligns with the UK Data Protection Laws applies.

6.4 Nothing in the IDTA (including the Commercial Clauses or the Linked Agreement) limits or excludes either Party's liability to Relevant Data Subjects or to the ICO under this IDTA or under UK Data Protection Laws.

6.5 If any wording in Parts one, two or three contradicts the Mandatory Clauses, and/or seeks to limit or exclude any liability to Relevant Data Subjects or to the ICO, then that wording will not apply.

6.6 The Parties may include provisions in the Linked Agreement which provide the Parties with enhanced rights otherwise covered by this IDTA. These enhanced rights may be subject to commercial terms, including payment, under the Linked Agreement, but this will not affect the rights granted under this IDTA.

6.7 If there is any inconsistency or conflict between this IDTA and a Linked Agreement or any other agreement, this IDTA overrides that Linked Agreement or any other agreements, even if those agreements have been negotiated by the Parties. The exceptions to this are where (and in so far as):

6.7.1 the inconsistent or conflicting terms of the Linked Agreement or other agreement provide greater protection for the Relevant Data Subject's rights, in which case those terms will override the IDTA; and

6.7.2 a Party acts as Processor and the inconsistent or conflicting terms of the Linked Agreement are obligations on that Party expressly required by Article 28 UK GDPR, in which case those terms will override the

inconsistent or conflicting terms of the IDTA in relation to Processing by that Party as Processor.

- 6.8 The words “include”, “includes”, “including”, “in particular” are used to set out examples and not to set out a finite list.
- 6.9 References to:
 - 6.9.1 singular or plural words or people, also includes the plural or singular of those words or people;
 - 6.9.2 legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this IDTA has been signed; and
 - 6.9.3 any obligation not to do something, includes an obligation not to allow or cause that thing to be done by anyone else.

7. Which laws apply to this IDTA

- 7.1 This IDTA is governed by the laws of the UK country set out in Table 2: Transfer Details. If no selection has been made, it is the laws of England and Wales. This does not apply to Section 35 which is always governed by the laws of England and Wales.

How this IDTA provides Appropriate Safeguards

8. The Appropriate Safeguards

- 8.1 The purpose of this IDTA is to ensure that the Transferred Data has Appropriate Safeguards when Processed by the Importer during the Term. This standard is met when and for so long as:
 - 8.1.1 both Parties comply with the IDTA, including the Security Requirements and any Extra Protection Clauses; and
 - 8.1.2 the Security Requirements and any Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach, including considering any Special Category Data within the Transferred Data.
- 8.2 The Exporter must:
 - 8.2.1 ensure and demonstrate that this IDTA (including any Security Requirements and Extra Protection Clauses) provides Appropriate Safeguards; and

8.2.2 (if the Importer reasonably requests) provide it with a copy of any TRA.

8.3 The Importer must:

8.3.1 before receiving any Transferred Data, provide the Exporter with all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including any information which may reasonably be required for the Exporter to carry out any TRA (the "Importer Information");

8.3.2 co-operate with the Exporter to ensure compliance with the Exporter's obligations under the UK Data Protection Laws;

8.3.3 review whether any Importer Information has changed, and whether any Local Laws contradict its obligations in this IDTA and take reasonable steps to verify this, on a regular basis. These reviews must be at least as frequent as the Review Dates; and

8.3.4 inform the Exporter as soon as it becomes aware of any Importer Information changing, and/or any Local Laws which may prevent or limit the Importer complying with its obligations in this IDTA. This information then forms part of the Importer Information.

8.4 The Importer must ensure that at the Start Date and during the Term:

8.4.1 the Importer Information is accurate;

8.4.2 it has taken reasonable steps to verify whether there are any Local Laws which contradict its obligations in this IDTA or any additional information regarding Local Laws which may be relevant to this IDTA.

8.5 Each Party must ensure that the Security Requirements and Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

9. Reviews to ensure the Appropriate Safeguards continue

9.1 Each Party must:

9.1.1 review this IDTA (including the Security Requirements and Extra Protection Clauses and the Importer Information) at regular intervals, to ensure that the IDTA remains accurate and up to date and continues to provide the Appropriate Safeguards. Each Party will carry out these reviews as frequently as the relevant Review Dates or sooner; and

- 9.1.2 inform the other party in writing as soon as it becomes aware if any information contained in either this IDTA, any TRA or Importer Information is no longer accurate and up to date.
- 9.2 If, at any time, the IDTA no longer provides Appropriate Safeguards the Parties must Without Undue Delay:
 - 9.2.1 pause transfers and Processing of Transferred Data whilst a change to the Tables is agreed. The Importer may retain a copy of the Transferred Data during this pause, in which case the Importer must carry out any Processing required to maintain, so far as possible, the measures it was taking to achieve the Appropriate Safeguards prior to the time the IDTA no longer provided Appropriate Safeguards, but no other Processing;
 - 9.2.2 agree a change to Part one: Tables or Part two: Extra Protection Clauses which will maintain the Appropriate Safeguards (in accordance with Section 5); and
 - 9.2.3 where a change to Part one: Tables or Part two: Extra Protection Clauses which maintains the Appropriate Safeguards cannot be agreed, the Exporter must end this IDTA by written notice on the Importer.

10. The ICO

- 10.1 Each Party agrees to comply with any reasonable requests made by the ICO in relation to this IDTA or its Processing of the Transferred Data.
- 10.2 The Exporter will provide a copy of any TRA, the Importer Information and this IDTA to the ICO, if the ICO requests.
- 10.3 The Importer will provide a copy of any Importer Information and this IDTA to the ICO, if the ICO requests.

The Exporter

11. Exporter's obligations

- 11.1 The Exporter agrees that UK Data Protection Laws apply to its Processing of the Transferred Data, including transferring it to the Importer.
- 11.2 The Exporter must:
 - 11.2.1 comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;
 - 11.2.2 comply with the Linked Agreement as it relates to its transferring the Transferred Data to the Importer; and
 - 11.2.3 carry out reasonable checks on the Importer's ability to comply with this IDTA, and take appropriate action including under Section 9.2,

Section 29 or Section 30, if at any time it no longer considers that the Importer is able to comply with this IDTA or to provide Appropriate Safeguards.

- 11.3 The Exporter must comply with all its obligations in the IDTA, including any in the Security Requirements, and any Extra Protection Clauses and any Commercial Clauses.
- 11.4 The Exporter must co-operate with reasonable requests of the Importer to pass on notices or other information to and from Relevant Data Subjects or any Third Party Controller where it is not reasonably practical for the Importer to do so. The Exporter may pass these on via a third party if it is reasonable to do so.
- 11.5 The Exporter must co-operate with and provide reasonable assistance to the Importer, so that the Importer is able to comply with its obligations to the Relevant Data Subjects under Local Law and this IDTA.

The Importer

12. General Importer obligations

- 12.1 The Importer must:
 - 12.1.1 only Process the Transferred Data for the Purpose;
 - 12.1.2 comply with all its obligations in the IDTA, including in the Security Requirements, any Extra Protection Clauses and any Commercial Clauses;
 - 12.1.3 comply with all its obligations in the Linked Agreement which relate to its Processing of the Transferred Data;
 - 12.1.4 keep a written record of its Processing of the Transferred Data, which demonstrate its compliance with this IDTA, and provide this written record if asked to do so by the Exporter;
 - 12.1.5 if the Linked Agreement includes rights for the Exporter to obtain information or carry out an audit, provide the Exporter with the same rights in relation to this IDTA; and
 - 12.1.6 if the ICO requests, provide the ICO with the information it would be required on request to provide to the Exporter under this Section 12.1 (including the written record of its Processing, and the results of audits and inspections).
- 12.2 The Importer must co-operate with and provide reasonable assistance to the Exporter and any Third Party Controller, so that the Exporter and any Third Party Controller are able to comply with their obligations under UK Data Protection Laws and this IDTA.

13. Importer's obligations if it is subject to the UK Data Protection Laws

13.1 If the Importer's Processing of the Transferred Data is subject to UK Data Protection Laws, it agrees that:

13.1.1 UK Data Protection Laws apply to its Processing of the Transferred Data, and the ICO has jurisdiction over it in that respect; and

13.1.2 it has and will comply with the UK Data Protection Laws in relation to the Processing of the Transferred Data.

13.2 If Section 13.1 applies and the Importer complies with Section 13.1, it does not need to comply with:

- Section 14 (Importer's obligations to comply with key data protection principles);
- Section 15 (What happens if there is an Importer Personal Data Breach);
- Section 15 (How Relevant Data Subjects can exercise their data subject rights); and
- Section 21 (How Relevant Data Subjects can exercise their data subject rights – if the Importer is the Exporter's Processor or Sub-Processor).

14. Importer's obligations to comply with key data protection principles

14.1 The Importer does not need to comply with this Section 14 if it is the Exporter's Processor or Sub-Processor.

14.2 The Importer must:

14.2.1 ensure that the Transferred Data it Processes is adequate, relevant and limited to what is necessary for the Purpose;

14.2.2 ensure that the Transferred Data it Processes is accurate and (where necessary) kept up to date, and (where appropriate considering the Purposes) correct or delete any inaccurate Transferred Data it becomes aware of Without Undue Delay; and

14.2.3 ensure that it Processes the Transferred Data for no longer than is reasonably necessary for the Purpose.

15. What happens if there is an Importer Personal Data Breach

15.1 If there is an Importer Personal Data Breach, the Importer must:

15.1.1 take reasonable steps to fix it, including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again. If the Importer is the Exporter's Processor or Sub-Processor: these steps must comply with the Exporter's instructions and

the Linked Agreement and be in co-operation with the Exporter and any Third Party Controller; and

- 15.1.2 ensure that the Security Requirements continue to provide (or are changed in accordance with this IDTA so they do provide) a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

15.2 If the Importer is a Processor or Sub-Processor: if there is an Importer Personal Data Breach, the Importer must:

- 15.2.1 notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

- 15.2.1.1 a description of the nature of the Importer Personal Data Breach;

- 15.2.1.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;

- 15.2.1.3 likely consequences of the Importer Personal Data Breach;

- 15.2.1.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;

- 15.2.1.5 contact point for more information; and

- 15.2.1.6 any other information reasonably requested by the Exporter,

- 15.2.2 if it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay; and

- 15.2.3 assist the Exporter (and any Third Party Controller) so the Exporter (or any Third Party Controller) can inform Relevant Data Subjects or the ICO or any other relevant regulator or authority about the Importer Personal Data Breach Without Undue Delay.

15.3 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a risk to the rights or freedoms of any Relevant Data Subject the Importer must notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

- 15.3.1 a description of the nature of the Importer Personal Data Breach;

- 15.3.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;
- 15.3.3 likely consequences of the Importer Personal Data Breach;
- 15.3.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;
- 15.3.5 contact point for more information; and
- 15.3.6 any other information reasonably requested by the Exporter.

If it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay.

- 15.4 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a high risk to the rights or freedoms of any Relevant Data Subject, the Importer must inform those Relevant Data Subjects Without Undue Delay, except in so far as it requires disproportionate effort, and provided the Importer ensures that there is a public communication or similar measures whereby Relevant Data Subjects are informed in an equally effective manner.
- 15.5 The Importer must keep a written record of all relevant facts relating to the Importer Personal Data Breach, which it will provide to the Exporter and the ICO on request.

This record must include the steps it takes to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Security Requirements continue to provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

16. Transferring on the Transferred Data

- 16.1 The Importer may only transfer on the Transferred Data to a third party if it is permitted to do so in Table 2: Transfer Details Table, the transfer is for the Purpose, the transfer does not breach the Linked Agreement, and one or more of the following apply:
 - 16.1.1 the third party has entered into a written contract with the Importer containing the same level of protection for Data Subjects as contained in this IDTA (based on the role of the recipient as controller or processor), and the Importer has conducted a risk assessment to ensure that the Appropriate Safeguards will be protected by that contract; or

- 16.1.2 the third party has been added to this IDTA as a Party; or
 - 16.1.3 if the Importer was in the UK, transferring on the Transferred Data would comply with Article 46 UK GDPR; or
 - 16.1.4 if the Importer was in the UK transferring on the Transferred Data would comply with one of the exceptions in Article 49 UK GDPR; or
 - 16.1.5 the transfer is to the UK or an Adequate Country.
- 16.2 The Importer does not need to comply with Section 16 if it is transferring on Transferred Data and/or allowing access to the Transferred Data in accordance with Section 23 (Access Requests and Direct Access).
- 17. Importer's responsibility if it authorises others to perform its obligations**
- 17.1 The Importer may sub-contract its obligations in this IDTA to a Processor or Sub-Processor (provided it complies with Section 16).
 - 17.2 If the Importer is the Exporter's Processor or Sub-Processor: it must also comply with the Linked Agreement or be with the written consent of the Exporter.
 - 17.3 The Importer must ensure that any person or third party acting under its authority, including a Processor or Sub-Processor, must only Process the Transferred Data on its instructions.
 - 17.4 The Importer remains fully liable to the Exporter, the ICO and Relevant Data Subjects for its obligations under this IDTA where it has sub-contracted any obligations to its Processor and Sub-Processor or authorised an employee or other person to perform them (and references to the Importer in this context will include references to its Processors, Sub-Processors or authorised persons).

What rights do individuals have?

18. The right to a copy of the IDTA

- 18.1 If a Party receives a request from a Relevant Data Subject for a copy of this IDTA:
 - 18.1.1 it will provide the IDTA to the Relevant Data Subject and inform the other Party, as soon as reasonably possible;
 - 18.1.2 it does not need to provide copies of the Linked Agreement, but it must provide all the information from those Linked Agreements referenced in the Tables;
 - 18.1.3 it may redact information in the Tables or the information provided from the Linked Agreement if it is reasonably necessary to protect business

secrets or confidential information, so long as it provides the Relevant Data Subject with a summary of those redactions so that the Relevant Data Subject can understand the content of the Tables or the information provided from the Linked Agreement.

19. The right to Information about the Importer and its Processing

19.1 The Importer does not need to comply with this Section 19 if it is the Exporter's Processor or Sub-Processor.

19.2 The Importer must ensure that each Relevant Data Subject is provided with details of:

- the Importer (including contact details and the Importer Data Subject Contact);
- the Purposes; and
- any recipients (or categories of recipients) of the Transferred Data;

The Importer can demonstrate it has complied with this Section 19.2 if the information is given (or has already been given) to the Relevant Data Subjects by the Exporter or another party.

The Importer does not need to comply with this Section 19.2 in so far as to do so would be impossible or involve a disproportionate effort, in which case, the Importer must make the information publicly available.

19.3 The Importer must keep the details of the Importer Data Subject Contact up to date and publicly available. This includes notifying the Exporter in writing of any such changes.

19.4 The Importer must make sure those contact details are always easy to access for all Relevant Data Subjects and be able to easily communicate with Data Subjects in the English language Without Undue Delay.

20. How Relevant Data Subjects can exercise their data subject rights

20.1 The Importer does not need to comply with this Section 0 if it is the Exporter's Processor or Sub-Processor.

20.2 If an individual requests, the Importer must confirm whether it is Processing their Personal Data as part of the Transferred Data.

20.3 The following Sections of this Section 20, relate to a Relevant Data Subject's Personal Data which forms part of the Transferred Data the Importer is Processing.

20.4 If the Relevant Data Subject requests, the Importer must provide them with a copy of their Transferred Data:

- 20.4.1 Without Undue Delay (and in any event within one month);
 - 20.4.2 at no greater cost to the Relevant Data Subject than it would be able to charge if it were subject to the UK Data Protection Laws;
 - 20.4.3 in clear and plain English that is easy to understand; and
 - 20.4.4 in an easily accessible form
- together with
- 20.4.5 (if needed) a clear and plain English explanation of the Transferred Data so that it is understandable to the Relevant Data Subject; and
 - 20.4.6 information that the Relevant Data Subject has the right to bring a claim for compensation under this IDTA.
- 20.5 If a Relevant Data Subject requests, the Importer must:
- 20.5.1 rectify inaccurate or incomplete Transferred Data;
 - 20.5.2 erase Transferred Data if it is being Processed in breach of this IDTA;
 - 20.5.3 cease using it for direct marketing purposes; and
 - 20.5.4 comply with any other reasonable request of the Relevant Data Subject, which the Importer would be required to comply with if it were subject to the UK Data Protection Laws.
- 20.6 The Importer must not use the Transferred Data to make decisions about the Relevant Data Subject based solely on automated processing, including profiling (the "Decision-Making"), which produce legal effects concerning the Relevant Data Subject or similarly significantly affects them, except if it is permitted by Local Law and:
- 20.6.1 the Relevant Data Subject has given their explicit consent to such Decision-Making; or
 - 20.6.2 Local Law has safeguards which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK; or
 - 20.6.3 the Extra Protection Clauses provide safeguards for the Decision-Making which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK.

21. How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter’s Processor or Sub-Processor

21.1 Where the Importer is the Exporter’s Processor or Sub-Processor: If the Importer receives a request directly from an individual which relates to the Transferred Data it must pass that request on to the Exporter Without Undue Delay. The Importer must only respond to that individual as authorised by the Exporter or any Third Party Controller.

22. Rights of Relevant Data Subjects are subject to the exemptions in the UK Data Protection Laws

22.1 The Importer is not required to respond to requests or provide information or notifications under Sections 18, 19, 20, 21 and 23 if:

22.1.1 it is unable to reasonably verify the identity of an individual making the request; or

22.1.2 the requests are manifestly unfounded or excessive, including where requests are repetitive. In that case the Importer may refuse the request or may charge the Relevant Data Subject a reasonable fee; or

22.1.3 a relevant exemption would be available under UK Data Protection Laws, were the Importer subject to the UK Data Protection Laws.

If the Importer refuses an individual’s request or charges a fee under Section 22.1.2 it will set out in writing the reasons for its refusal or charge, and inform the Relevant Data Subject that they are entitled to bring a claim for compensation under this IDTA in the case of any breach of this IDTA.

How to give third parties access to Transferred Data under Laws

23. Access requests and direct access

23.1 In this Section 23 an “Access Request” is a legally binding request (except for requests only binding by contract law) to access any Transferred Data and “Direct Access” means direct access to any Transferred Data by public authorities of which the Importer is aware.

23.2 The Importer may disclose any requested Transferred Data in so far as it receives an Access Request, unless in the circumstances it is reasonable for it to challenge that Access Request on the basis there are significant grounds to believe that it is unlawful.

23.3 In so far as Local Laws allow and it is reasonable to do so, the Importer will Without Undue Delay provide the following with relevant information about any Access Request or Direct Access: the Exporter; any Third Party Controller; and where the Importer is a Controller, any Relevant Data Subjects.

23.4 In so far as Local Laws allow, the Importer must:

- 23.4.1 make and keep a written record of Access Requests and Direct Access, including (if known): the dates, the identity of the requestor/accessor, the purpose of the Access Request or Direct Access, the type of data requested or accessed, whether it was challenged or appealed, and the outcome; and the Transferred Data which was provided or accessed; and
- 23.4.2 provide a copy of this written record to the Exporter on each Review Date and any time the Exporter or the ICO reasonably requests.

24. Giving notice

- 24.1 If a Party is required to notify any other Party in this IDTA it will be marked for the attention of the relevant Key Contact and sent by e-mail to the e-mail address given for the Key Contact.
- 24.2 If the notice is sent in accordance with Section 24.1, it will be deemed to have been delivered at the time the e-mail was sent, or if that time is outside of the receiving Party's normal business hours, the receiving Party's next normal business day, and provided no notice of non-delivery or bounceback is received.
- 24.3 The Parties agree that any Party can update their Key Contact details by giving 14 days' (or more) notice in writing to the other Party.

25. General clauses

- 25.1 In relation to the transfer of the Transferred Data to the Importer and the Importer's Processing of the Transferred Data, this IDTA and any Linked Agreement:
 - 25.1.1 contain all the terms and conditions agreed by the Parties; and
 - 25.1.2 override all previous contacts and arrangements, whether oral or in writing.
- 25.2 If one Party made any oral or written statements to the other before entering into this IDTA (which are not written in this IDTA) the other Party confirms that it has not relied on those statements and that it will not have a legal remedy if those statements are untrue or incorrect, unless the statement was made fraudulently.
- 25.3 Neither Party may novate, assign or obtain a legal charge over this IDTA (in whole or in part) without the written consent of the other Party, which may be set out in the Linked Agreement.

- 25.4 Except as set out in Section 17.1, neither Party may sub contract its obligations under this IDTA without the written consent of the other Party, which may be set out in the Linked Agreement.
- 25.5 This IDTA does not make the Parties a partnership, nor appoint one Party to act as the agent of the other Party.
- 25.6 If any Section (or part of a Section) of this IDTA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity and enforceability of any other Section (or the rest of that Section) of this IDTA.
- 25.7 If a Party does not enforce, or delays enforcing, its rights or remedies under or in relation to this IDTA, this will not be a waiver of those rights or remedies. In addition, it will not restrict that Party's ability to enforce those or any other right or remedy in future.
- 25.8 If a Party chooses to waive enforcing a right or remedy under or in relation to this IDTA, then this waiver will only be effective if it is made in writing. Where a Party provides such a written waiver:
- 25.8.1 it only applies in so far as it explicitly waives specific rights or remedies;
 - 25.8.2 it shall not prevent that Party from exercising those rights or remedies in the future (unless it has explicitly waived its ability to do so); and
 - 25.8.3 it will not prevent that Party from enforcing any other right or remedy in future.

What happens if there is a breach if this IDTA?

26. Breaches of this IDTA

- 26.1 Each Party must notify the other Party in writing (and with all relevant details) if it:
- 26.1.1 has breached this IDTA; or
 - 26.1.2 it should reasonably anticipate that it may breach this IDTA, and provide any information about this which the other Party reasonably requests.
- 26.2 In this IDTA "Significant Harmful Impact" means that there is more than a minimal risk of a breach of the IDTA causing (directly or indirectly) significant damage to any Relevant Data Subject or the other Party.

27. Breaches of this IDTA by the Importer

- 27.1 If the Importer has breached this IDTA, and this has a Significant Harmful Impact, the Importer must take steps Without Undue Delay to end the Significant Harmful Impact, and if that is not possible to reduce the Significant Harmful Impact as much as possible.
- 27.2 Until there is no ongoing Significant Harmful Impact on Relevant Data Subjects:
 - 27.2.1 the Exporter must suspend sending Transferred Data to the Importer;
 - 27.2.2 If the Importer is the Exporter's Processor or Sub-Processor: if the Exporter requests, the importer must securely delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter); and
 - 27.2.3 if the Importer has transferred on the Transferred Data to a third party receiver under Section 16, and the breach has a Significant Harmful Impact on Relevant Data Subject when it is Processed by or on behalf of that third party receiver, the Importer must:
 - 27.2.3.1 notify the third party receiver of the breach and suspend sending it Transferred Data; and
 - 27.2.3.2 if the third party receiver is the Importer's Processor or Sub-Processor: make the third party receiver securely delete all Transferred Data being Processed by it or on its behalf, or securely return it to the Importer (or a third party named by the Importer).
- 27.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Exporter must end this IDTA under Section 30.1.

28. Breaches of this IDTA by the Exporter

- 28.1 If the Exporter has breached this IDTA, and this has a Significant Harmful Impact, the Exporter must take steps Without Undue Delay to end the Significant Harmful Impact and if that is not possible to reduce the Significant Harmful Impact as much as possible.
- 28.2 Until there is no ongoing risk of a Significant Harmful Impact on Relevant Data Subjects, the Exporter must suspend sending Transferred Data to the Importer.
- 28.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Importer must end this IDTA under Section 30.1.

Ending the IDTA

29. How to end this IDTA without there being a breach

29.1 The IDTA will end:

- 29.1.1 at the end of the Term stated in Table 2: Transfer Details; or
- 29.1.2 if in Table 2: Transfer Details, the Parties can end this IDTA by providing written notice to the other: at the end of the notice period stated;
- 29.1.3 at any time that the Parties agree in writing that it will end; or
- 29.1.4 at the time set out in Section 29.2.

29.2 If the ICO issues a revised Approved IDTA under Section 5.4, if any Party selected in Table 2 "Ending the IDTA when the Approved IDTA changes", will as a direct result of the changes in the Approved IDTA have a substantial, disproportionate and demonstrable increase in:

- 29.2.1 its direct costs of performing its obligations under the IDTA; and/or
- 29.2.2 its risk under the IDTA,

and in either case it has first taken reasonable steps to reduce that cost or risk so that it is not substantial and disproportionate, that Party may end the IDTA at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved IDTA.

30. How to end this IDTA if there is a breach

30.1 A Party may end this IDTA immediately by giving the other Party written notice if:

- 30.1.1 the other Party has breached this IDTA and this has a Significant Harmful Impact. This includes repeated minor breaches which taken together have a Significant Harmful Impact, and
 - 30.1.1.1 the breach can be corrected so there is no Significant Harmful Impact, and the other Party has failed to do so Without Undue Delay (which cannot be more than 14 days of being required to do so in writing); or
 - 30.1.1.2 the breach and its Significant Harmful Impact cannot be corrected;
- 30.1.2 the Importer can no longer comply with Section 8.3, as there are Local Laws which mean it cannot comply with this IDTA and this has a Significant Harmful Impact.

31. What must the Parties do when the IDTA ends?

- 31.1 If the parties wish to bring this IDTA to an end or this IDTA ends in accordance with any provision in this IDTA, but the Importer must comply with a Local Law which requires it to continue to keep any Transferred Data then this IDTA will remain in force in respect of any retained Transferred Data for as long as the retained Transferred Data is retained, and the Importer must:
- 31.1.1 notify the Exporter Without Undue Delay, including details of the relevant Local Law and the required retention period;
 - 31.1.2 retain only the minimum amount of Transferred Data it needs to comply with that Local Law, and the Parties must ensure they maintain the Appropriate Safeguards, and change the Tables and Extra Protection Clauses, together with any TRA to reflect this; and
 - 31.1.3 stop Processing the Transferred Data as soon as permitted by that Local Law and the IDTA will then end and the rest of this Section 29 will apply.
- 31.2 When this IDTA ends (no matter what the reason is):
- 31.2.1 the Exporter must stop sending Transferred Data to the Importer; and
 - 31.2.2 if the Importer is the Exporter's Processor or Sub-Processor: the Importer must delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter), as instructed by the Exporter;
 - 31.2.3 if the Importer is a Controller and/or not the Exporter's Processor or Sub-Processor: the Importer must securely delete all Transferred Data.
 - 31.2.4 the following provisions will continue in force after this IDTA ends (no matter what the reason is):
 - **Section 1** (This IDTA and Linked Agreements);
 - **Section 2** (Legal Meaning of Words);
 - **Section 6** (Understanding this IDTA);
 - **Section 7** (Which laws apply to this IDTA);
 - **Section 10** (The ICO);
 - Sections 11.1 and 11.4 (Exporter's obligations);
 - Sections 12.1.2, 12.1.3, 12.1.4, and 12.1.5 and 12.1.6 (General Importer obligations);

- Section 13.1 (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 17** (Importer's responsibility if it authorised others to perform its obligations);
- **Section 24** (Giving notice);
- **Section 25** (General clauses);
- **Section 31** (What must the Parties do when the IDTA ends);
- **Section 32** (Your liability);
- **Section 33** (How Relevant Data Subjects and the ICO may bring legal claims);
- **Section 34** (Courts legal claims can be brought in);
- **Section 35** (Arbitration); and
- **Section 36** (Legal Glossary).

How to bring a legal claim under this IDTA

32. Your liability

32.1 The Parties remain fully liable to Relevant Data Subjects for fulfilling their obligations under this IDTA and (if they apply) under UK Data Protection Laws.

32.2 Each Party (in this Section, "Party One") agrees to be fully liable to Relevant Data Subjects for the entire damage suffered by the Relevant Data Subject, caused directly or indirectly by:

32.2.1 Party One's breach of this IDTA; and/or

32.2.2 where Party One is a Processor, Party One's breach of any provisions regarding its Processing of the Transferred Data in the Linked Agreement;

32.2.3 where Party One is a Controller, a breach of this IDTA by the other Party if it involves Party One's Processing of the Transferred Data (no matter how minimal)

in each case unless Party One can prove it is not in any way responsible for the event giving rise to the damage.

32.3 If one Party has paid compensation to a Relevant Data Subject under Section 32.2, it is entitled to claim back from the other Party that part of the

compensation corresponding to the other Party's responsibility for the damage, so that the compensation is fairly divided between the Parties.

32.4 The Parties do not exclude or restrict their liability under this IDTA or UK Data Protection Laws, on the basis that they have authorised anyone who is not a Party (including a Processor) to perform any of their obligations, and they will remain responsible for performing those obligations.

33. How Relevant Data Subjects and the ICO may bring legal claims

33.1 The Relevant Data Subjects are entitled to bring claims against the Exporter and/or Importer for breach of the following (including where their Processing of the Transferred Data is involved in a breach of the following by either Party):

- **Section 1** (This IDTA and Linked Agreements);
- **Section 3** (You have provided all the information required by Part one: Tables and Part two: Extra Protection Clauses);
- **Section 8** (The Appropriate Safeguards);
- **Section 9** (Reviews to ensure the Appropriate Safeguards continue);
- **Section 11** (Exporter's obligations);
- **Section 12** (General Importer Obligations);
- **Section 13** (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 14** (Importer's obligations to comply with key data protection laws);
- **Section 15** (What happens if there is an Importer Personal Data Breach);
- **Section 16** (Transferring on the Transferred Data);
- **Section 17** (Importer's responsibility if it authorises others to perform its obligations);
- **Section 18** (The right to a copy of the IDTA);
- **Section 19** (The Importer's contact details for the Relevant Data Subjects);
- **Section 20** (How Relevant Data Subjects can exercise their data subject rights);
- **Section 21** (How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor);
- **Section 23** (Access Requests and Direct Access);

- **Section 26** (Breaches of this IDTA);
- **Section 27** (Breaches of this IDTA by the Importer);
- **Section 28** (Breaches of this IDTA by the Exporter);
- **Section 30** (How to end this IDTA if there is a breach);
- **Section 31** (What must the Parties do when the IDTA ends); and
- any other provision of the IDTA which expressly or by implication benefits the Relevant Data Subjects.

33.2 The ICO is entitled to bring claims against the Exporter and/or Importer for breach of the following Sections: Section 10(The ICO), Sections 11.1 and 11.2 (Exporter's obligations), Section 12.1.6 (General Importer obligations) and Section 13 (Importer's obligations if it is subject to UK Data Protection Laws).

33.3 No one else (who is not a Party) can enforce any part of this IDTA (including under the Contracts (Rights of Third Parties) Act 1999).

33.4 The Parties do not need the consent of any Relevant Data Subject or the ICO to make changes to this IDTA, but any changes must be made in accordance with its terms.

33.5 In bringing a claim under this IDTA, a Relevant Data Subject may be represented by a not-for-profit body, organisation or association under the same conditions set out in Article 80(1) UK GDPR and sections 187 to 190 of the Data Protection Act 2018.

34. Courts legal claims can be brought in

34.1 The courts of the UK country set out in Table 2: Transfer Details have non-exclusive jurisdiction over any claim in connection with this IDTA (including non-contractual claims).

34.2 The Exporter may bring a claim against the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.

34.3 The Importer may only bring a claim against the Exporter in connection with this IDTA (including non-contractual claims) in the courts of the UK country set out in the Table 2: Transfer Details

34.4 Relevant Data Subjects and the ICO may bring a claim against the Exporter and/or the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.

34.5 Each Party agrees to provide to the other Party reasonable updates about any claims or complaints brought against it by a Relevant Data Subject or the ICO in connection with the Transferred Data (including claims in arbitration).

35. Arbitration

35.1 Instead of bringing a claim in a court under section 34, any Party, or a Relevant Data Subject may elect to refer any dispute arising out of or in connection with this IDTA (including non-contractual claims) to final resolution by arbitration under the Rules of the London Court of International Arbitration, and those Rules are deemed to be incorporated by reference into this Section 35.

35.2 The Parties agree to submit to any arbitration started by another Party or by a Relevant Data Subject in accordance with this Section 35.

35.3 There must be only one arbitrator. The arbitrator (1) must be a lawyer qualified to practice law in one or more of England and Wales, or Scotland, or Northern Ireland and (2) must have experience of acting or advising on disputes relating to UK Data Protection Laws.

35.4 London shall be the seat or legal place of arbitration. It does not matter if the Parties selected a different UK country as the 'primary place for legal claims to be made' in Table 2: Transfer Details.

35.5 The English language must be used in the arbitral proceedings.

35.6 English law governs this Section 35. This applies regardless of whether or not the parties selected a different UK country's law as the 'UK country's law that governs the IDTA' in Table 2: Transfer Details.

36. Legal Glossary

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Access Request	As defined in Section 23, as a legally binding request (except for requests only binding by contract law) to access any Transferred Data.
Adequate Country	A third country, or: <ul style="list-style-type: none">• a territory;• one or more sectors or organisations within a third country;

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
	<ul style="list-style-type: none"> an international organisation; <p>which the Secretary of State has specified by regulations provides an adequate level of protection of Personal Data in accordance with Section 17A of the Data Protection Act 2018.</p>
Appropriate Safeguards	The standard of protection over the Transferred Data and of the Relevant Data Subject's rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved IDTA	The template IDTA A1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4.
Commercial Clauses	The commercial clauses set out in Part three.
Controller	As defined in the UK GDPR.
Damage	All material and non-material loss and damage.
Data Subject	As defined in the UK GDPR.
Decision-Making	As defined in Section 20.6, as decisions about the Relevant Data Subjects based solely on automated processing, including profiling, using the Transferred Data.
Direct Access	As defined in Section 23 as direct access to any Transferred Data by public authorities of which the Importer is aware.
Exporter	The exporter identified in Table 1: Parties & Signature.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Extra Protection Clauses	The clauses set out in Part two: Extra Protection Clauses.
ICO	The Information Commissioner.
Importer	The importer identified in Table 1: Parties & Signature.
Importer Data Subject Contact	The Importer Data Subject Contact identified in Table 1: Parties & Signature, which may be updated in accordance with Section 19.
Importer Information	As defined in Section 8.3.1, as all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including for the Exporter to carry out any TRA.
Importer Personal Data Breach	A 'personal data breach' as defined in UK GDPR, in relation to the Transferred Data when Processed by the Importer.
Linked Agreement	The linked agreements set out in Table 2: Transfer Details (if any).
Local Laws	Laws which are not the laws of the UK and which bind the Importer.
Mandatory Clauses	Part four: Mandatory Clauses of this IDTA.
Notice Period	As set out in Table 2: Transfer Details.
Party/Parties	The parties to this IDTA as set out in Table 1: Parties & Signature.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Personal Data	As defined in the UK GDPR.
Personal Data Breach	As defined in the UK GDPR.
Processing	As defined in the UK GDPR. When the IDTA refers to Processing by the Importer, this includes where a third party Sub-Processor of the Importer is Processing on the Importer's behalf.
Processor	As defined in the UK GDPR.
Purpose	The 'Purpose' set out in Table 2: Transfer Details, including any purposes which are not incompatible with the purposes stated or referred to.
Relevant Data Subject	A Data Subject of the Transferred Data.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR
Review Dates	The review dates or period for the Security Requirements set out in Table 2: Transfer Details, and any review dates set out in any revised Approved IDTA.
Significant Harmful Impact	As defined in Section 26.2 as where there is more than a minimal risk of the breach causing (directly or indirectly) significant harm to any Relevant Data Subject or the other Party.
Special Category Data	As described in the UK GDPR, together with criminal conviction or criminal offence data.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Start Date	As set out in Table 1: Parties and signature.
Sub-Processor	A Processor appointed by another Processor to Process Personal Data on its behalf. This includes Sub-Processors of any level, for example a Sub-Sub-Processor.
Tables	The Tables set out in Part one of this IDTA.
Term	As set out in Table 2: Transfer Details.
Third Party Controller	The Controller of the Transferred Data where the Exporter is a Processor or Sub-Processor If there is not a Third Party Controller this can be disregarded.
Transfer Risk Assessment or TRA	A risk assessment in so far as it is required by UK Data Protection Laws to demonstrate that the IDTA provides the Appropriate Safeguards
Transferred Data	Any Personal Data which the Parties transfer, or intend to transfer under this IDTA, as described in Table 2: Transfer Details
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in Section 3 of the Data Protection Act 2018.
Without Undue Delay	Without undue delay, as that phrase is interpreted in the UK GDPR.

Alternative Part 4 Mandatory Clauses:

Mandatory Clauses	Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.
--------------------------	--

SCHEDULE 5 – SECURITY REQUIREMENTS AND PLAN

INTERPRETATION AND DEFINITION

For the purposes of this Schedule 5, unless the context otherwise requires the following provisions shall have the meanings given to them below:

“Breach of Security” means the occurrence of unauthorised access to or use of the Premises, the Premises, the Services, the Contractor System, or any ICT or data (including Authority Data) used by the Authority or the Contractor in connection with the Contract.

“Contractor Equipment” means the hardware, computer and telecoms devices and equipment supplied by the Contractor or its Sub-Contractor (but not hired, leased or loaned from the Authority) for the provision of the Services;

“Contractor Software” means software, which is proprietary to the Contractor, including software which is or will be used by the Contractor for the purposes of providing the Services.

“ICT” means Information Communications Technology and includes a diverse set of technological tools and resources used to communicate, and to create, disseminate, store and manage information, including computers, the Internet, broadcasting technologies (radio and television), and telephony.

“Security Plan” means the Contractor’s Global Information Security Policy set forth at the following link: <https://ddiworld.com/gisp>.

“Software” means Tools, Contractor Software and Third-Party Software.

“Specially Written Software” NOT APPLICABLE.

“Third Party Software” means software which is proprietary to any third party and licensed to Contractor and may be used by the Contractor for the purposes of providing the Services.

1. INTRODUCTION

This Schedule 5 covers:

- 1.1 principles of security for the Contractor System, including without limitation principles of physical and information security;
- 1.2 wider aspects of security relating to the Services;
- 1.3 the creation of the Security Plan;
- 1.4 audit and testing of the Security Plan; and
- 1.5 breaches of security.

2. PRINCIPLES OF SECURITY

- 2.1 The Contractor acknowledges that the Authority places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Premises and the security for the Contractor System. The Contractor also acknowledges the confidentiality of Authority Data.
- 2.2 The Contractor shall be responsible for the security of the Contractor System and shall at all times provide a level of security which:
 - 2.2.1 is in accordance with Good Industry Practice and Law;
 - 2.2.2 meets any specific security threats to the Contractor System.
- 2.3 Without limiting paragraph 2.2, the Contractor shall at all times ensure that the level of security employed in the provision of the Services is appropriate to maintain the following at acceptable risk levels (to be defined by the Authority):
 - 2.3.1 loss of integrity of Authority Data;
 - 2.3.2 loss of confidentiality of Authority Data;
 - 2.3.3 unauthorised access to, use of, or interference with Authority Data by any person or organisation;
 - 2.3.4 unauthorised access to network elements, buildings, the Premises, and tools used by the Contractor in the provision of the Services;
 - 2.3.5 use of the Contractor System or Services by any third party in order to gain unauthorised access to any computer resource or Authority Data; and
 - 2.3.6 loss of availability of Authority Data due to any failure or compromise of the Services.
 - 2.3.7 processing and storage of authority data within the UK or by exception within the EEA. Any processing outside of the UK must be subject to specific approval by the Authority. The foregoing notwithstanding, the Authority acknowledges that all of Contractor's data servers are located in the United States and thus all data will be transferred to and processed in the United States.

3. SECURITY PLAN

- 3.1 The Contractor shall develop, implement and maintain a Security Plan to apply during the Contract Period (and after the end of the term as applicable) details of which are available here: <https://ddiworld.com/gisp>
- 3.2 The Security Plan will set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the Services and all processes associated with the delivery of the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with:
 - 3.2.1 the provisions of this Schedule 5;
 - 3.2.2 the provisions of Schedule 1 relating to security;

- 3.2.3 the data protection compliance guidance produced by the Authority;
 - 3.2.4 the minimum set of security measures and standards required where the system will be handling Protectively Marked or sensitive information, as determined by the Security Policy Framework;
 - 3.2.5 any other extant national information security requirements and guidance, as provided by the Authority's IT security officers; and
 - 3.2.6 appropriate ICT standards for technical countermeasures which are included in the Contractor System.
- 3.3 The references to Quality Standards, guidance and policies set out in this Schedule shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such Quality Standards, guidance and policies, from time to time.
- 3.4 If there is any inconsistency in the provisions of the above standards, guidance and policies, the Contractor should notify the Authorised Representative of such inconsistency immediately upon becoming aware of the same, and the Authorised Representative shall, as soon as practicable, advise the Contractor which provision the Contractor shall be required to comply with.
- 3.5 The Security Plan will be structured in accordance with ISO/IEC27002 and ISO/IEC27001 or other equivalent policy or procedure, cross-referencing if necessary, to other schedules of the Contract which cover specific areas included within that standard.
- 3.6 The Security Plan shall not reference any other documents which are not either in the possession of the Authority or otherwise specified in this Schedule 5.

4. AMENDMENT AND REVISION

- 4.1 The Security Plan will be fully reviewed and updated by the Contractor annually or from time to time to reflect:
- 4.1.1 emerging changes in Good Industry Practice;
 - 4.1.2 any change or proposed change to the Contractor System, the Services and/or associated processes;
 - 4.1.3 any new perceived or changed threats to the Contractor System;
 - 4.1.4 changes to security policies introduced Government-wide or by the Authority; and/or
 - 4.1.5 a reasonable request by the Authority.
- 4.2 The Contractor will provide the Authority with an executive summary of the results of such reviews as soon as reasonably practicable after their completion and amend the Security Plan at no additional cost to the Authority.

5. AUDIT, TESTING AND PROTECTIVE MONITORING NOT USED

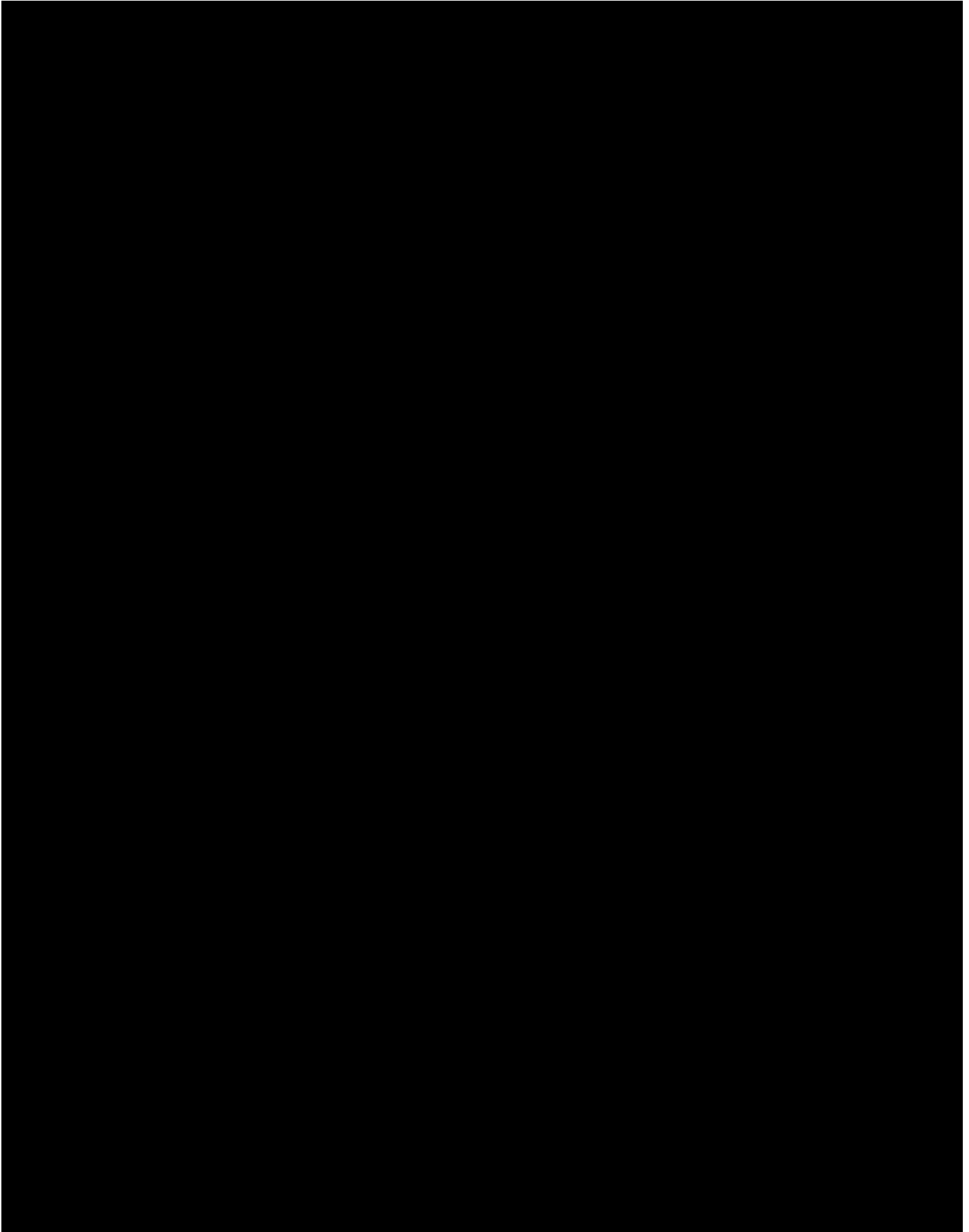
6. BREACH OF SECURITY

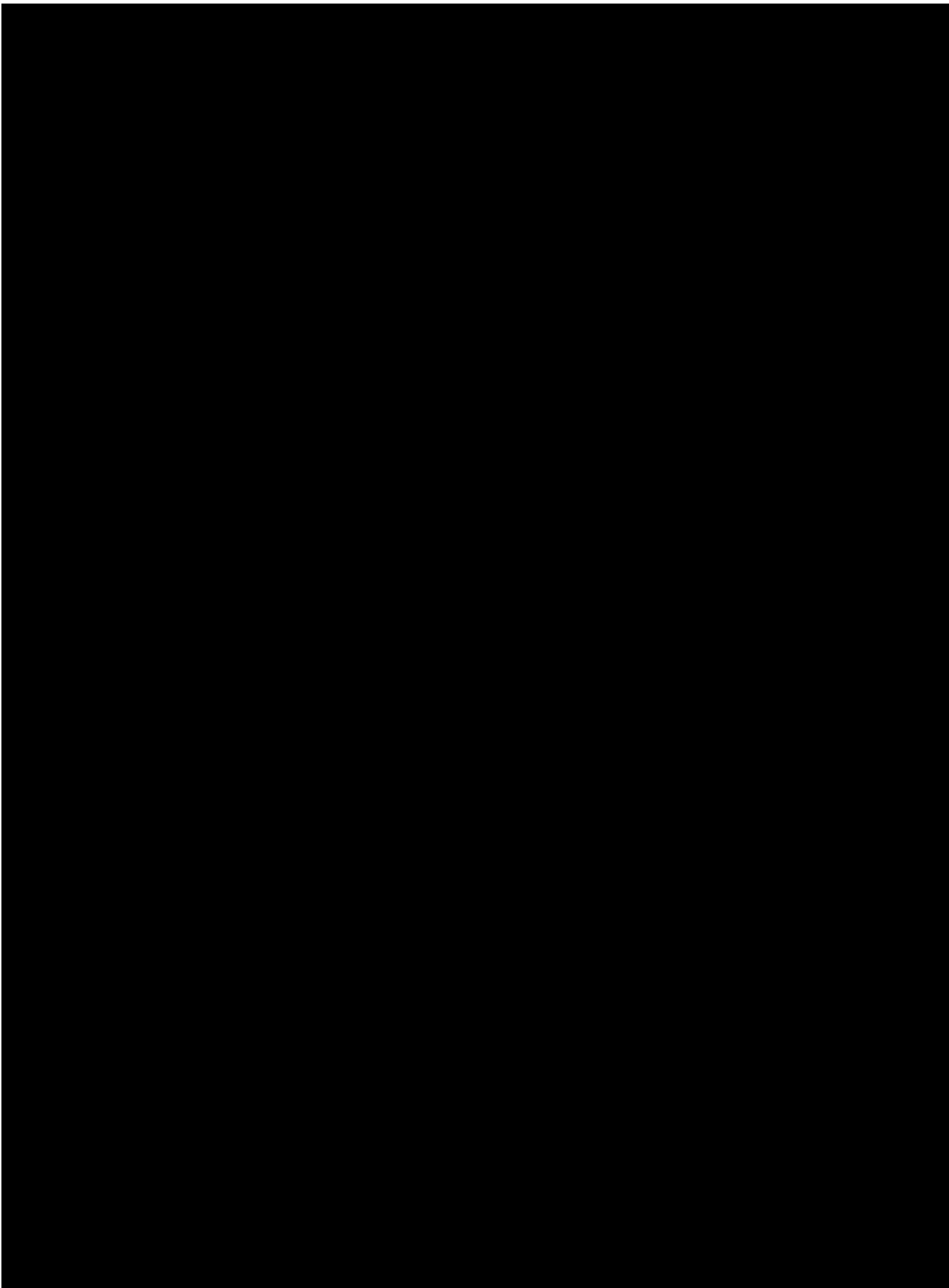
- 6.1 Either Party shall notify the other without undue delay upon becoming aware of any Breach of Security.
- 6.2 Upon becoming aware of any of the circumstances referred to in paragraph 6.1, the Contractor shall without undue delay take all reasonable steps necessary to:
- 6.2.1 remedy such breach or protect the Contractor System against any such potential or attempted breach or threat; and
 - 6.2.2 prevent an equivalent breach in the future;
 - 6.2.3 collect, preserve and protect all available audit data relating to the incident and make it available on request to the Authority;
 - 6.2.4 investigate the incident and produce a detailed report for the Authority without undue delay.
- 6.3 Such steps shall include any action or changes reasonably required by the Authority. If such action is taken in response to a breach that is determined by the Authority acting reasonably not to be covered by the obligations of the Contractor under the Contract, then the Contractor shall be entitled to refer the matter to the variation procedure set out in the Contract.
- 6.4 The Contractor shall as soon as reasonably practicable provide to the Authority full details (using such reporting mechanism as may be specified by the Authority from time to time) of any Security Breach and of the steps taken in respect thereof.

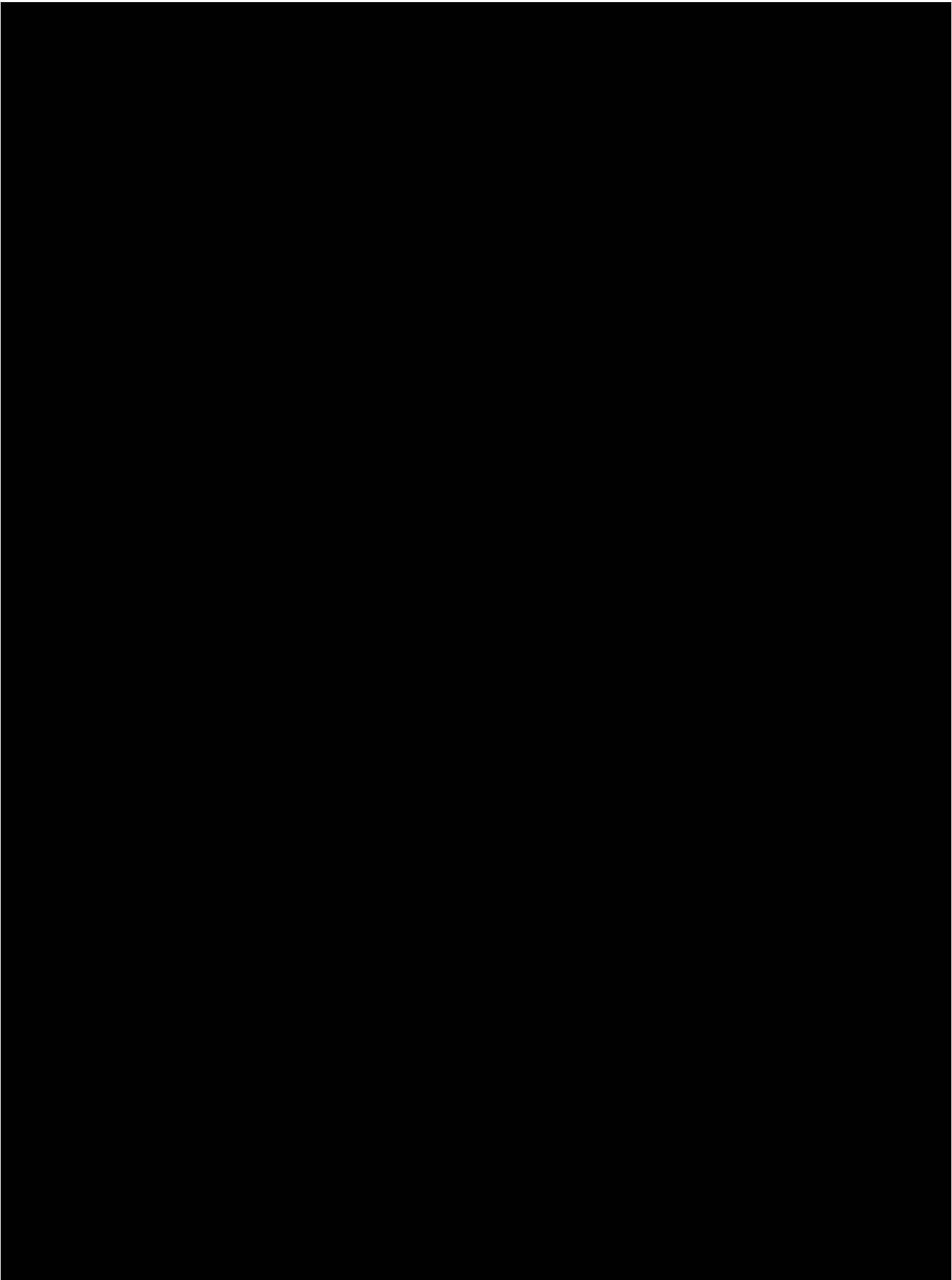
7. CONTRACT EXIT – SECURITY REQUIREMENTS

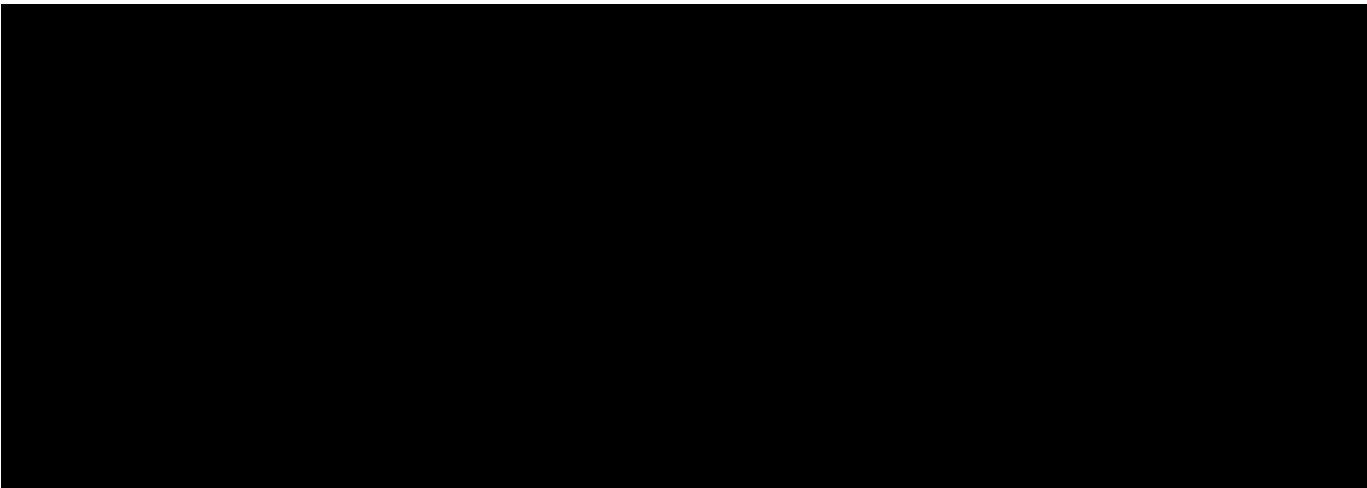
In accordance with clause 16 of the Contract, on termination of the Contract, either via early termination or completion of the Contract then the Contractor will either return all data to the Authority or provide a certificate of secure destruction using an industry and Authority approved method. Destruction or return of the data will be specified by the Authority at the time of termination of the Contract.

APPENDIX 1- OUTLINE SECURITY PLAN

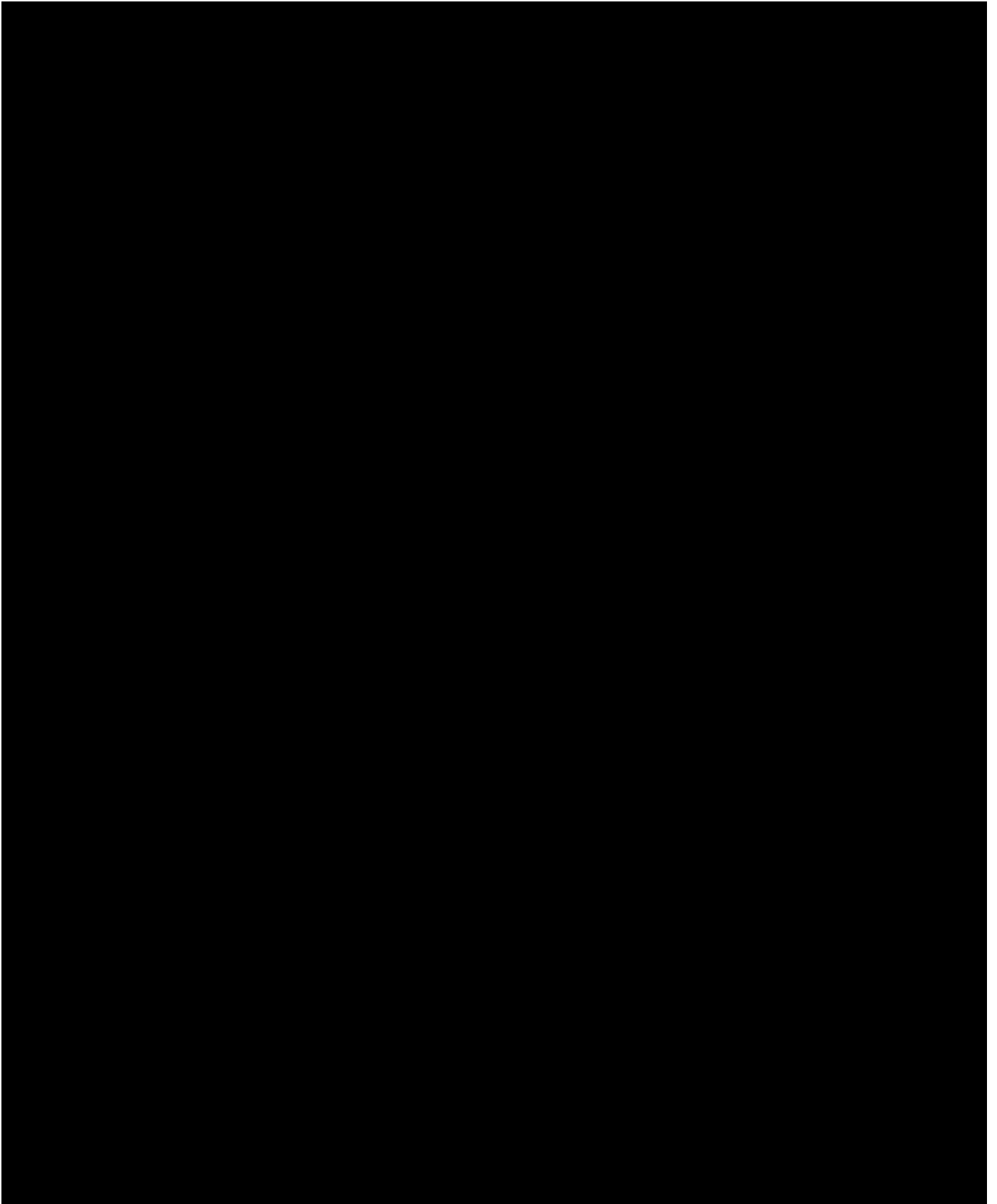








ANNEX 2: CONTRACTOR'S SECURITY MANAGEMENT PLAN



SCHEDULE 6 – CHANGE CONTROL

Contract Change Note

Contract Change Note Number	
Contract Reference Number & Title	
Variation Title	
Number of Pages	

WHEREAS the Contractor and the Authority entered into a Contract for the supply of [project name] dated [dd/mm/yyyy] (the "Original Contract") and now wish to amend the Original Contract

IT IS AGREED as follows

1. The Original Contract shall be amended as set out in this Change Control Notice:

Change Requestor / Originator		
Summary of Change		
Reason for Change		
Revised Contract Price	Original Contract Value	£
	Previous Contract Changes	£
	Contract Change Note [x]	£
	New Contract Value	£
Revised Payment Schedule		
Revised Specification (See Annex [x] for Details)		
Revised Term/Contract Period		
Change in Contract Manager(s)		
Other Changes		

2. Save as herein amended all other terms of the Original Contract shall remain effective.
3. This Change Control Notice shall take effect on

SIGNED ON BEHALF OF THE AUTHORITY:	SIGNED ON BEHALF OF THE CONTRACTOR:
Signature:	Signature:
Name:	Name:
Position:	Position:
Date:	Date:

SCHEDULE 7 – THIRD PARTY SOFTWARE – NOT USED

CONTRACTOR SOFTWARE

For the purposes of this Schedule 7, “**Contractor Software**” means software which is proprietary to the Contractor, including software which is or will be used by the Contractor for the purposes of providing the Services. The Contractor Software comprises the following items:

Software	Contractor (if Affiliate of the Contractor)	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?

THIRD PARTY SOFTWARE

For the purposes of this Schedule 7, “**Third Party Software**” means software which is proprietary to any third party which is or will be used by the Contractor for the purposes of providing the Services including the software specified in this Schedule 7. The Third-Party Software shall consist of the following items:

Third Party Software	Contractor	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?

SCHEDULE 8 – EXIT MANAGEMENT STRATEGY

Exit management will be agreed by both parties.