**Annex A**

**Conditions**

# **DEFINITIONS USED IN THE BUYER CONTRACT**

1. In this Buyer Contract, unless the context otherwise requires, the following words shall have the following meanings:

|  |  |
| --- | --- |
| **“Buyer”** | means the person identified in the letterhead of the Letter; |
| **"Buyer Cause"** | any breach of the obligations of the Buyer or any other default, act, omission, negligence or statement of the Buyer, of its employees, servants, agents in connection with or in relation to the subject-matter of the Buyer Contract and in respect of which the Buyer is liable to the Supplier; |
| **“Buyer Contract”** | has the meaning given to it in the Letter; |
| **“CCS”** | the Minister for the Cabinet Office as represented by Crown Commercial Service, which is an executive agency and operates as a trading fund of the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool L3 9PP; |
|  |  |
| **"Central Government Body"** | 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:   1. Government Department; 2. Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); 3. Non-Ministerial Department; or 4. Executive Agency; |
| **"Charges"** | means the charges specified in Part 2 of Annex F and which in aggregate shall in no circumstances exceed the thresholds set out in regulation 5 of the Regulations; |
| **“Commercially Sensitive Information”** | the Confidential Information listed in the email of acceptance comprising of commercially sensitive information relating to the Supplier, its intellectual property rights or its business or which the Supplier has indicated to the Buyer that, if disclosed by the Buyer, would cause the Supplier significant commercial disadvantage or material financial loss; |
| **"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; |
| **"Controller"** | has the meaning given to it in the UK GDPR; |
| **"Data Protection Impact Assessment"** | an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data; |
| **"Data Protection Legislation"** | (i) the UK GDPR, as amended from time to time, (ii) the Data Protection Act 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy; |
| **"Data Protection Officer"** | has the meaning given to it in the UK GDPR; |
| **"Data Subject"** | has the meaning given to it in the UK GDPR; |
| **"Data Subject Access**  **Request"** | 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; |
| **"Deliver"** | means hand over the Deliverables to the Buyer at the address and on the date specified in Annex C, which shall include unloading and any other specific arrangements agreed in any Special Term. “**Delivered**”, “**Deliveries**” and “**Delivery**” shall be construed accordingly; |
| **“Deliverables”** | Offered Deliverables that are ordered under the Buyer Contract and described in Part 1 of Annex F; |
| **“DOTAS”** | the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions; |
| **“Electronic Invoice”** | an invoice which has been issued, transmitted and received in a structured electronic format which allows for its automatic and electronic processing and which complies with (a) the European standard and (b) any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870; |
| **"Existing IPR"** | any and all intellectual property rights that are owned by or licensed to either Party and which have been developed independently of the Buyer Contract (whether prior to the date of the Buyer Contract or otherwise); |
| **"Expiry Date"** | means the date for expiry of the Buyer Contract as set out in the Letter; |
| **"FOIA"** | means the Freedom of Information Act 2000 together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation; |
| **"Force Majeure Event"** | any event, occurrence, circumstance, matter or cause affecting the performance by either the Buyer or the Supplier of its obligations arising from acts, events, omissions, happenings or non-happenings beyond the reasonable control of the affected Party which prevent or materially delay the affected Party from performing its obligations under the Buyer Contract and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by the affected Party, including:  a) riots, civil commotion, war or armed conflict;  b) acts of terrorism;  c) acts of a Central Government Body, local government or regulatory bodies;  d) fire, flood, storm or earthquake or other natural disaster,  but excluding any industrial dispute relating to the Supplier, the Supplier Staff, or any other failure in the Supplier or the subcontractor's supply chain; |
| **"General Anti-Abuse Rule"** | a) the legislation in Part 5 of the Finance Act 2013; and  b) any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements to avoid National Insurance contributions; |
| **"Goods"** | means the goods to be supplied by the Supplier to the Buyer under the Buyer Contract; |
| **"Good Industry Practice"** | standards, practices, methods and procedures conforming to the Law and the exercise of 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 within the relevant industry or business sector; |
| **"Government Data"** | 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, including any of the Buyer's confidential information, and which: i) are supplied to the Supplier by or on behalf of the Buyer; or ii) the Supplier is required to generate, process, store or transmit pursuant to the Buyer Contract; or b) any Personal Data for which the Buyer is the Data Controller; |
| **“Halifax Abuse Principle”** | the principle explained in the CJEU Case C-255/02 Halifax and others; |
| “**Independent Control**” | where a Controller has provided Personal Data to another Party which is not a Processor or a Joint Controller because the recipient itself determines the purposes and means of Processing but does so separately from the Controller providing it with Personal Data and “**Independent Controller**” shall be construed accordingly; |
| **"Information"** | has the meaning given under section 84 of the FOIA; |
| **"Information Commissioner"** | the UK’s independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies; |
| **"Insolvency Event"** | in respect of a person: a) if that person is insolvent; ii) if an order is made or a resolution is passed for the winding up of the person (other than voluntarily for the purpose of solvent amalgamation or reconstruction); iii) if an administrator or administrative receiver is appointed in respect of the whole or any part of the persons assets or business; iv) if the person makes any composition with its creditors or takes or suffers any similar or analogous action to any of the actions detailed in this definition as a result of debt in any jurisdiction; |
| **“IR35”** | the off-payroll rules requiring individuals who work through their company pay the same tax and National Insurance contributions as an employee which can be found online at: <https://www.gov.uk/guidance/ir35-find-out-if-it-applies>; |
| **“Joint Controller Agreement”** | the agreement (if any) entered into between the Buyer and the Supplier substantially in the form set out in Appendix 2 of Annex D; |
| **“Joint Control”** | where two or more Controllers jointly determine the purposes and means of Processing and “**Joint Controller**” shall be construed accordingly; |
| **“Law”** | 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, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply; |
| **“Letter”** | the letter from the Buyer to the Supplier offering to enter into the Buyer Contract; |
| **“Losses”** | all losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise; |
| **“LVPS”** | has the meaning given to it in the Letter; |
| **“LVPS Contract”** | the contract between CCS and the Supplier for the admission of the Supplier to the LVPS pursuant to which the Supplier makes the Offered Deliverables available for sale under this Buyer Contract; |
| **“Maximum Liability Amount”** | the amount specified in Annex C of the Letter; |
| **“Minimum Warranty Period”** | the minimum period for which the Supplier warrants the Deliverables specified in Annex C of Letter; |
| **"New IPR"** | all intellectual property rights in any materials created or developed by or on behalf of the Supplier pursuant to the Buyer Contract but shall not include the Supplier's Existing IPR; |
| **“Occasion of Tax Non-Compliance”** | where:  a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which is found on or after 1 April 2013 to be incorrect as a result of:  i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation in any jurisdiction that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle;  ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime in any jurisdiction; and/or  b) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for tax related offences which is not spent at the first day of the Term or to a civil penalty for fraud or evasion; |
| **"Offered Deliverables"** | Goods and/or Services which meet the description of the service heading relating to the Deliverables and the location of the Deliverables as detailed in the LVPS; |
| **"Party"** | the Supplier or the Buyer (as appropriate) and "Parties" shall mean both of them; |
| **"Personal Data"** | has the meaning given to it in the UK GDPR; |
| **"Personal Data Breach"** | has the meaning given to it in the UK GDPR; |
| “**Processing**” | has the meaning given to it in the UK GDPR; |
| **"Processor"** | has the meaning given to it in the UK GDPR; |
| **“Processor Personnel”** | all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under the Buyer Contract; |
| **“Prohibited Acts”** | a) to directly or indirectly offer, promise or give any person working for or engaged by the Buyer or any other public body a financial or other advantage to:  i) induce that person to perform improperly a relevant function or activity; or  ii) 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 Buyer Contract; or  c) committing any offence:  i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or  ii) under legislation or common law concerning fraudulent acts; or  iii) defrauding, attempting to defraud or conspiring to defraud the Buyer or other public body; or  d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK; |
| **“Protective Measures”** | appropriate technical and organisational measures 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; |
| **"Purchase Order Number"** | means the Buyer’s unique number relating to the order for Deliverables to be supplied by the Supplier to the Buyer in accordance with the terms of the Buyer Contract; |
| **“Recall”** | a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the right intellectual property rights) that might endanger health or hinder performance; |
| **“Relevant Requirements”** | applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State pursuant to section 9 of the Bribery Act 2010; |
| **“Relevant Tax Authority”** | HMRC, or, if applicable, the tax authority in the jurisdiction in which the Supplier is established; |
| **"Regulations"** | the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires) as amended from time to time; |
| **"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); |
| **"Services"** | means the services to be supplied by the Supplier to the Buyer under the Buyer Contract; |
| **“Special Term”** | any special term specified in Annex B to the Letter; |
| **"Staff Vetting Procedures"** | means vetting procedures that accord with good industry practice or, where applicable, the Buyer’s procedures for the vetting of personnel as provided to the Supplier from time to time; |
| **“Suitability Assessment Questionnaire”** | The questionnaire completed by the Supplier as part of its application for inclusion in the LVPS, as set out at Annex E; |
| **"Subprocessor"** | any third Party appointed to process Personal Data on behalf of the Supplier related to the Buyer Contract; |
| **"Supplier Staff"** | all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any subcontractor engaged in the performance of the Supplier’s obligations under the Buyer Contract; |
| **"Supplier"** | means the person named as Supplier in the Letter; |
| **"Term"** | means the period from the start date of the Buyer Contract identified in paragraph 6 of the Letter to the Expiry Date as such period may be extended in accordance with paragraph 6 of the Letter or terminated in accordance with the terms and conditions of the Buyer Contract; |
| **“Transparency Information”** | the content of the Buyer Contract, including any changes to the Buyer Contract agreed from time to time, except for:  (i) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Buyer; and    (ii) Commercially Sensitive Information; |
| **"UK GDPR"** | the retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679); |
| **"VAT"** | means value added tax in accordance with the provisions of the Value Added Tax Act 1994; |
| **"Workers"** | any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (<https://www.gov.uk/government/publications/procurement-policynote-0815-tax-arrangements-of-appointees>) applies in respect of the Deliverables; and |
| **"Working Day"** | means a day (other than a Saturday or Sunday) on which banks are open for business in the City of London. |

# **UNDERSTANDING THE BUYER CONTRACT**

In the Buyer Contract, unless the context otherwise requires:

## references to numbered clauses are references to the relevant clause in these terms and conditions;

## 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;

## the headings in this Buyer Contract are for information only and do not affect the interpretation of the Buyer Contract;

## references to "writing" include printing, display on a screen and electronic transmission and other modes of representing or reproducing words in a visible form;

## the singular includes the plural and vice versa;

## a reference to any law includes a reference to that law as amended, extended, consolidated or re-enacted from time to time and to any legislation or byelaw made under that law; and

## the word ‘including’, "for example" and similar words shall be understood as if they were immediately followed by the words "without limitation".

# **HOW THE BUYER CONTRACT WORKS**

## Any Special Terms that the Buyer has included in Annex B supplement or change these Conditions.

## This Buyer Contract is a separate contract from the LVPS Contract and survives the termination of the LVPS Contract.

## The Supplier acknowledges it has all the information required to perform its obligations under the Buyer Contract before entering into the Buyer Contract. When information is provided by the Buyer no warranty of its accuracy is given to the Supplier.

## The Supplier will not be excused from any obligation, or be entitled to additional Charges because it failed to either:

### verify the accuracy of any information provided to the Supplier by or on behalf of the Buyer prior to the first day of the Term; or

### properly perform its own adequate checks.

## The Buyer will not be liable for errors, omissions or misrepresentation of any information.

## The Supplier warrants and represents all statements made and documents submitted as part of the procurement of Deliverables are and remain true and accurate.

## The Buyer and the Supplier acknowledge and agree that the Buyer awarded this Buyer Contract to the Supplier pursuant to Part 4 of the Regulations and that as such the value of this Buyer Contract, including any form of option, any renewal and any modifications, shall be less than the relevant threshold mentioned in Regulation 5 of the Regulations.

# **WHAT NEEDS TO BE DELIVERED**

## **All Deliverables**

### The Supplier must provide Deliverables:

### in accordance with the Offered Deliverables;

### to a professional standard;

### using reasonable skill and care;

### using Good Industry Practice;

### using its own policies, processes and internal quality control measures as long as they do not conflict with the Buyer Contract;

### on the dates agreed; and

### that comply with all Law.

### The Supplier must provide Deliverables with a warranty of at least the Minimum Warranty Period (or longer where the Supplier offers a longer warranty period to its Buyers) from Delivery against all obvious defects.

### The Supplier must assign all third party warranties and indemnities covering the Deliverables for the Buyer's benefit.

## **Goods clauses**

### All Goods delivered must be new, or as new if recycled, unused and of recent origin.

### All manufacturer warranties covering the Goods must be assignable to the Buyer on request and for free.

### The Supplier transfers ownership of the Goods on completion of Delivery or payment for those Goods, whichever is earlier.

### Risk in the Goods transfers to the Buyer on Delivery of the Goods, but remains with the Supplier if the Buyer notices damage following Delivery and lets the Supplier know within three Working Days of Delivery.

### The Supplier warrants that it has full and unrestricted ownership of the Goods at the time of transfer of ownership.

### The Supplier must Deliver the Goods on the date and to the specified location during the Buyer's working hours.

### The Supplier must provide sufficient packaging for the Goods to reach the point of Delivery safely and undamaged.

### All Deliveries must have a delivery note attached that specifies the order number, type and quantity of Goods.

### The Supplier must provide all tools, information and instructions the Buyer needs to make use of the Goods.

### The Supplier must indemnify the Buyer against the costs of any Recall of the Goods and will give notice of actual or anticipated action about the Recall of the Goods.

### The Buyer can cancel any order or part order of Goods which has not been Delivered. If the Buyer gives less than 14 days' notice then it will pay the Supplier's reasonable and proven costs already incurred on the cancelled order as long as the Supplier takes all reasonable steps to minimise these costs.

### The Supplier must at its own cost repair, replace, refund or substitute (at the Buyer's option and request) any Goods that the Buyer rejects because they do not conform with clause 4.2. If the Supplier does not do this it will pay the Buyer's costs including repair or re-supply by a third party.

## **Services clauses**

### Late Delivery of the Services will be a default of the Buyer Contract.

### The Supplier must co-operate with the Buyer and third party suppliers on all aspects connected with the Delivery of the Services and ensure that Supplier Staff comply with any reasonable instructions.

### The Supplier must at its own risk and expense provide all equipment required to Deliver the Services.

### The Supplier must allocate sufficient resources and appropriate expertise to the Buyer Contract.

### The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer's operations, employees or other contractors.

### The Supplier must ensure all Services, and anything used to Deliver the Services, are of good quality and free from defects.

### The Buyer is entitled to withhold payment for partially or undelivered Services, but doing so does not stop it from using its other rights under the Buyer Contract.

# **PRICING AND PAYMENTS**

## In exchange for the Deliverables, the Supplier shall be entitled to invoice the Buyer for the Charges. The Supplier shall raise invoices promptly and in any event within 90 days from when the Charges are due.

## All Charges:

### exclude VAT, which is payable on provision of a valid VAT invoice;

### include all costs connected with the supply of Deliverables.

## The Buyer must pay the Supplier the Charges within 30 days of receipt by the Buyer of a valid, undisputed invoice, in cleared funds to the Supplier's account stated in the email accepting the Buyer Contract.

## A Supplier invoice is only valid if it:

### includes all appropriate references including the Purchase Order Number and other details reasonably requested by the Buyer;

### includes a detailed breakdown of Deliverables which have been Delivered (if any); and

### does not include any Management Charge (the Supplier must not charge the Buyer in any way for the Management Charge).

## The Buyer must accept and process for payment an undisputed Electronic Invoice received from the Supplier.

## The Buyer may retain or set-off payment of any amount owed to it by the Supplier if notice and reasons are provided.

## 

## The Supplier must ensure that all subcontractors are paid, in full, within 30 days of receipt of a valid, undisputed invoice. If this does not happen, the Buyer can publish the details of the late payment or non-payment.

## The Supplier has no right of set-off, counterclaim, discount or abatement unless they are ordered to do so by a court.

# **THE BUYER'S OBLIGATIONS TO THE SUPPLIER**

## 

## If the Supplier fails to comply with the Buyer Contract as a result of a Buyer Cause:

### the Buyer cannot terminate the Buyer Contract under clause 11;

### the Supplier is entitled to reasonable and proven additional expenses and to relief from liability under this Buyer Contract;

### the Supplier is entitled to additional time needed to Deliver the Deliverables; and

### the Supplier cannot suspend the ongoing supply of Deliverables.

## Clause 6.1 only applies if the Supplier:

### gives notice to the Buyer within 10 Working Days of becoming aware;

### demonstrates that the failure would not have occurred but for the Buyer Cause; and

### mitigated the impact of the Buyer Cause.

# **RECORD KEEPING AND REPORTING**

## The Supplier must ensure that suitably qualified representatives attend progress meetings with the Buyer and provide progress reports when specified in Annex C to the Letter.

## The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Buyer Contract:

## during the term of the Buyer Contract;

## for seven years after the date of expiry or termination of the Buyer Contract; and

* + 1. in accordance with UK GDPR.

## The Buyer or an auditor can audit the Supplier.

## The Supplier must allow any auditor appointed by the Buyer access to their premises to verify all contract accounts and records of everything to do with the Buyer Contract and provide copies for the audit.

## The Supplier must provide information to the auditor and reasonable co-operation at their request.

## Where the audit of the Supplier is carried out by an auditor, the auditor shall be entitled to share any information obtained during the audit with the Buyer.

## If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:

### tell the Buyer and give reasons;

### propose corrective action; and

### provide a deadline for completing the corrective action.

## If the Buyer, acting reasonably, is concerned as to the financial stability of the Supplier such that it may impact on the continued performance of the Buyer Contract then the Buyer may:

### require that the Supplier provide to the Buyer (for its approval) a plan setting out how the Supplier will ensure continued performance of the Buyer Contract and the Supplier will make changes to such plan as reasonably required by the Buyer and once it is agreed then the Supplier shall act in accordance with such plan and report to the Buyer on demand; and

### if the Supplier fails to provide a plan or fails to agree any changes which are requested by the Buyer or fails to implement or provide updates on progress with the plan, terminate the Buyer Contract immediately for material breach (or on such date as the Buyer notifies).

# **SUPPLIER STAFF**

## The Supplier Staff involved in the performance of the Buyer Contract must:

### be appropriately trained and qualified;

### be vetted using Good Industry Practice and in accordance with the Staff Vetting Procedures; and

### comply with all conduct requirements when on the Buyer's premises.

## Where a Buyer decides one of the Supplier's Staff is not suitable to work on the Buyer Contract, the Supplier must replace them with a suitably qualified alternative.

## If requested, the Supplier must replace any person whose acts or omissions have caused the Supplier to breach clause 26.

## The Supplier must provide a list of Supplier Staff needing to access the Buyer's premises and say why access is required.

## The Supplier indemnifies the Buyer against all claims brought by any person employed by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.

## The Supplier shall use those persons nominated in the email of acceptance (if any) to provide the Deliverables and shall not remove or replace any of them unless:

### requested to do so by the Buyer (not to be unreasonably withheld or delayed);

### the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or

### the person's employment or contractual arrangement with the Supplier or any subcontractor is terminated for material breach of contract by the employee.

# **RIGHTS AND PROTECTION**

## The Supplier warrants and represents that:

### it has full capacity and authority to enter into and to perform the Buyer Contract;

### the Buyer Contract is executed by its authorised representative;

### it is a legally valid and existing organisation incorporated in the place it was formed;

### there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its affiliates that might affect its ability to perform the Buyer Contract;

### it maintains all necessary rights, authorisations, licences and consents to perform its obligations under the Buyer Contract;

### it does not have any contractual obligations which are likely to have a material adverse effect on its ability to perform the Buyer Contract; and

### it is not impacted by an Insolvency Event.

## The warranties and representations in clauses 3.6 and 9.1 are repeated each time the Supplier provides Deliverables under the Buyer Contract.

## The Supplier indemnifies the Buyer against each of the following:

### willful misconduct of the Supplier, any of its subcontractor and/or Supplier Staff that impacts the Buyer Contract; and

### non-payment by the Supplier of any tax or National Insurance.

## If the Supplier becomes aware of a representation or warranty that becomes untrue or misleading, it must immediately notify the Buyer.

# **INTELLECTUAL PROPERTY RIGHTS (IPRS)**

## Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable worldwide licence to use, change and sub-license the Supplier's Existing IPR to enable it and its sub-licensees to both:

### receive and use the Deliverables; and

### use the New IPR.

## 

## Any New IPR created under the Buyer Contract is owned by the Buyer. The Buyer gives the Supplier a licence to use any Existing IPRs for the purpose of fulfilling its obligations under the Buyer Contract and a perpetual, royalty-free, non-exclusive licence to use any New IPRs.

## Where a Party acquires ownership of intellectual property rights incorrectly under this Buyer Contract it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.

## Neither Party has the right to use the other Party's intellectual property rights, including any use of the other Party's names, logos or trademarks, except as provided in clause 10 or otherwise agreed in writing.

## If any claim is made against the Buyer 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 Deliverables (an "**IPR Claim**"), then the Supplier indemnifies the Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result of the IPR Claim.

## If an IPR Claim is made or anticipated the Supplier must at its own expense and the Buyer's sole option, either:

### obtain for the Buyer the rights in clauses 10.1 and 10.2 without infringing any third party intellectual property rights; or

### replace or modify the relevant item with substitutes that do not infringe intellectual property rights without adversely affecting the functionality or performance of the Deliverables.

## In spite of any other provisions of the Buyer Contract and for the avoidance of doubt, award of the Buyer Contract by the Buyer and placement of any contract task under it does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977 or Section 12 of the Registered Designs Act 1949. The Supplier acknowledges that any authorisation by the Buyer under its statutory powers must be expressly provided in writing with reference to the acts authorised.

# **ENDING THE CONTRACT**

## **Ending the Buyer Contract without a reason**

### The Buyer has the right to terminate the Buyer Contract at any time without reason or liability by giving the Supplier not less than 30 days' written notice.

## 

## **When the Buyer can end the Buyer Contract**

### If any of the following events happen, the Buyer has the right to immediately terminate the Buyer Contract by issuing a termination notice in writing to the Supplier:

#### there is a Supplier Insolvency Event;

#### if the Supplier is in breach of any obligation which is capable of remedy, and that breach is not remedied within 30 days of the Supplier receiving notice specifying the breach and requiring it to be remedied;

#### there is any material breach of the Buyer Contract;

#### there is a material default of any Joint Controller Agreement relating to the Buyer Contract;

#### there is a breach of clauses 3.6, 3.7, 10, 14, 15, 26 or 31;

#### if the Supplier repeatedly breaches the Buyer Contract in a way 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 Buyer Contract;

#### there's a change of control (within the meaning of section 450 of the Corporation Tax Act 2010) of the Supplier which is not pre-approved by the Buyer in writing;

#### if the Buyer discovers that the Supplier was in one of the situations set out in Section 2 of the Suitability Assessment Questionnaire at the time the Buyer Contract was awarded or is in breach of clause 26.1 of this Contract; or

#### the Supplier or its affiliates embarrass or bring the Buyer into disrepute or diminish the public trust in them.

### If any of the following non-fault based events happen, the Buyer has the right to immediately terminate the Buyer Contract:

### there is a change to the Buyer Contract which cannot be agreed using clause 24 or resolved using clause 33; or

### if there is a declaration of ineffectiveness in respect of any change to the Buyer Contract.

## **When the Supplier can end the Buyer Contract**

### The Supplier can issue a reminder notice if the Buyer does not pay an undisputed invoice on time. The Supplier can terminate the Buyer Contract if the Buyer fails to pay an undisputed invoiced sum due and worth over 10% of the total Buyer Contract value or £1,000, whichever is the lower, within 30 days of the date of the reminder notice.

## **What happens if the Buyer Contract ends**

### Where a Party terminates the Buyer Contract under any of clauses 11.1, 11.2(a), 11.2(b), 11.3, 20.2, 23.4 or 31.3 all of the following apply:

### the Buyer's payment obligations under the terminated Buyer Contract stop immediately;

### accumulated rights of the Parties are not affected;

### the Supplier must promptly repay to the Buyer any and all Charges the Buyer has paid in advance in respect of Deliverables not provided by the Supplier as at the termination date;

### the Supplier must promptly delete or return the Government Data except where required to retain copies by Law;

### the Supplier must promptly return any of the Buyer's property provided under the Buyer Contract;

### the Supplier must, at no cost to the Buyer, give all reasonable assistance to the Buyer and any incoming supplier and co-operate fully in the handover and re-procurement;

* + 1. In addition to the consequences of termination listed in clause 11.4(a), where the Buyer terminates the Buyer Contract under clause 11.2(a), the Supplier is responsible for the Buyer's reasonable costs of procuring replacement Deliverables for the rest of the term of the Buyer Contract.
    2. In addition to the consequences of termination listed in clause 11.4(a), if either the Buyer terminates the Buyer Contract under clause 11.1 or the Supplier terminates the Buyer Contract under either of clauses 11.3 or 23.4:

### the Buyer must promptly pay all outstanding Charges incurred to the Supplier; and

### the Buyer must pay the Supplier reasonable committed and unavoidable Losses as long as the Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Buyer Contract had not been terminated.

* + 1. In addition to the consequences of termination listed in clause 11.4(a), where a Party terminates under clause 20.2 each Party must cover its own Losses.

### The following clauses survive the termination of the Buyer Contract: 7, 8.5, 10, 12, 14, 15, 16, 17, 18, 33, 34 and any clauses which are expressly or by implication intended to continue.

## 

## **Partially ending and suspending the Buyer Contract**

### Where the Buyer has the right to terminate the Buyer Contract it can terminate or suspend (for any period), all or part of it. If the Buyer suspends the Buyer Contract it can provide the Deliverables itself or buy them from a third party.

### The Buyer can only partially terminate or suspend the Buyer Contract if the remaining parts of it can still be used to effectively deliver the intended purpose.

### The Parties must agree (in accordance with clause 24) any necessary variation required by clause 11.5, but the Supplier may not either:

#### reject the variation;

#### increase the Charges, except where the right to partial termination is under clause 11.1.

### The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under clause 11.5.

# **HOW MUCH YOU CAN BE HELD RESPONSIBLE FOR**

## Each Party's total aggregate liability under or in connection with the Buyer Contract (whether in tort, contract or otherwise) is no more than the higher of the Maximum Liability Amount or 150% of the Charges paid or payable to the Supplier.

## No Party is liable to the other for:

### any indirect Losses; or

### loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect).

## In spite of clause 12.1, neither Party limits or excludes any of the following:

### its liability for death or personal injury caused by its negligence, or that of its employees, agents or subcontractors;

### its liability for bribery or fraud or fraudulent misrepresentation by it or its employees;

### any liability that cannot be excluded or limited by Law; or

### its liability to the extent it arises as a result of a default by the Supplier, any fine or penalty incurred by the Buyer pursuant to Law and any costs incurred by the Buyer in defending any proceedings which result in such fine or penalty.

## Each Party must use all reasonable endeavours to mitigate any Loss or damage which it suffers under or in connection with the Buyer Contract, including any indemnities.

## If more than one Supplier is party to the Buyer Contract, each Supplier Party is jointly and severally liable for their obligations under the Buyer Contract.

# **OBEYING THE LAW**

## The Supplier must, in connection with provision of the Deliverables, use reasonable endeavours to:

### comply and procure that its subcontractors comply with the Supplier Code of Conduct appearing at ([https://www.gov.uk/government/uploads/system/uploads/attachment\_data/fi le/646497/2017-09- 13\_Official\_Sensitive\_Supplier\_Code\_of\_Conduct\_September\_2017.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/fi%20le/646497/2017-09-%2013_Official_Sensitive_Supplier_Code_of_Conduct_September_2017.pdf)) and such other corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time;

### support the Buyer in fulfilling its Public Sector Equality duty under S149 of the Equality Act 2010;

### not use nor allow its subcontractors to use modern slavery, child labour or inhumane treatment;

### meet the applicable Government Buying Standards applicable to Deliverables which can be found online at: <https://www.gov.uk/government/collections/sustainable-procurement-thegovernment-buying-standards-gbs>

# **DATA PROTECTION**

## The Supplier must process Personal Data and ensure that Supplier Staff process Personal Data only in accordance with Annex D of the Letter.

## The Supplier must not remove any ownership or security notices in or relating to the Government Data.

## The Supplier must make accessible back-ups of all Government Data, stored in an agreed off-site location and send the Buyer copies every six months.

## The Supplier must ensure that any Supplier system holding any Government Data, including back-up data, is a secure system that complies with the security requirements specified in writing by the Buyer.

## If at any time the Supplier suspects or has reason to believe that the Government Data provided under the Buyer Contract is corrupted, lost or sufficiently degraded, then the Supplier must notify the Buyer and immediately suggest remedial action.

## 

## If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Buyer may either or both:

### tell the Supplier to restore or get restored Government Data as soon as practical but no later than five Working Days from the date that the Buyer receives notice, or the Supplier finds out about the issue, whichever is earlier; and/or

### restore the Government Data itself or using a third party.

## The Supplier must pay each Party's reasonable costs of complying with clause 14.6 unless the Buyer is at fault.

## The Supplier:

### must provide the Buyer with all Government Data in an agreed open format within 10 Working Days of a written request;

### must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading;

### must securely destroy all Storage Media that has held Government Data at the end of life of that media using Good Industry Practice;

### securely erase all Government Data and any copies it holds when asked to do so by the Buyer unless required by Law to retain it; and

### indemnifies the Buyer against any and all Losses incurred if the Supplier breaches clause 14 and any Data Protection Legislation.

## In the event that, following the end of the UK’s transition period for exit from the EU, CCS determines in its absolute discretion that any of the Standard Contractual Clauses for data transfers issued by the European Commission from time to time applies to any Processing under or in connection with this Buyer Contract, at its own expense, each Party shall do everything necessary to give full effect to the relevant Standard Contractual Clauses as part of this Buyer Contract.

# **WHAT YOU MUST KEEP CONFIDENTIAL**

## Each Party must:

### keep all Confidential Information it receives confidential and secure;

### except as expressly set out in clauses 15.2 to 15.4 or elsewhere in the Buyer Contract, not disclose, use or exploit the disclosing Party's Confidential Information without the disclosing Party's prior written consent; and

### immediately notify the disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information.

## 

## In spite of clause 15.1, a Party may disclose Confidential Information which it receives from the disclosing Party in any of the following instances:

### where disclosure is required by applicable Law or by a court with the relevant jurisdiction if the recipient Party notifies the disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure;

### if the recipient Party already had the information without obligation of confidentiality before it was disclosed by the disclosing Party;

### if the information was given to it by a third party without obligation of confidentiality;

### if the information was in the public domain at the time of the disclosure;

### if the information was independently developed without access to the disclosing Party's Confidential Information;

### on a confidential basis, to its auditors;

### on a confidential basis, to its professional advisers on a need-to-know basis; or

### to the Serious Fraud Office where the recipient Party has reasonable grounds to believe that the disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010.

## In spite of clause 15.1, the Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Buyer Contract. The Supplier Staff must enter into a direct confidentiality agreement with the Buyer at its request.

## 

## In spite of clause 15.1, the Buyer may disclose Confidential Information in any of the following cases:

### on a confidential basis to the employees, agents, consultants and contractors of the Buyer;

### on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company that the Buyer transfers or proposes to transfer all or any part of its business to;

### if the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions;

### where requested by Parliament; or

### under clauses 5.8 and 16.

## For the purposes of clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in clause 15.

## Transparency Information is not Confidential Information.

## The Supplier must not make any press announcement or publicise the Buyer Contract or any part of it in any way, without the prior written consent of the Buyer and must take all reasonable steps to ensure that Supplier Staff do not either.

# 

# **WHEN YOU CAN SHARE INFORMATION**

## The Supplier must tell the Buyer within 48 hours if it receives a Request For Information.

## Within five (5) Working Days of the Buyer’s request the Supplier must give the Buyer full co-operation and information needed so the Buyer can:

### publish the Transparency Information;

### comply with any Freedom of Information Act (FOIA) request; and/or

### comply with any Environmental Information Regulations (EIR) request.

## The Buyer may talk to the Supplier to help it decide whether to publish information under clause 16. However, the extent, content and format of the disclosure is the Buyer’s decision, in its absolute discretion.

# **INVALID PARTS OF THE CONTRACT**

1. If any part of the Buyer Contract is prohibited by Law or judged by a court to be unlawful, void or unenforceable, it must be read as if it was removed from that Buyer Contract as much as required and rendered ineffective as far as possible without affecting the rest of the Buyer Contract, whether it is valid or enforceable.

# **NO OTHER TERMS APPLY**

1. The provisions incorporated into the Buyer Contract are the entire agreement between the Parties. The Buyer Contract replaces all previous statements, agreements and any course of dealings made between the Parties, whether written or oral, in relation to its subject matter. No other provisions apply.

# **OTHER PEOPLE'S RIGHTS IN A CONTRACT**

1. No third parties may use the Contracts (Rights of Third Parties) Act 1999 (“**CRTPA**”) to enforce any term of the Buyer Contract unless stated (referring to CRTPA) in the Buyer Contract. This does not affect third party rights and remedies that exist independently from CRTPA.

# **CIRCUMSTANCES BEYOND YOUR CONTROL**

## Any Party affected by a Force Majeure Event is excused from performing its obligations under the Buyer Contract while the inability to perform continues, if it both:

### provides written notice to the other Party; and

### uses all reasonable measures practical to reduce the impact of the Force Majeure Event.

## 

## Either Party can partially or fully terminate the Buyer Contract if the provision of the Deliverables is materially affected by a Force Majeure Event which lasts for 90 days continuously.

# **RELATIONSHIPS CREATED BY THE CONTRACT**

1. The Buyer Contract does not create a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

# **GIVING UP CONTRACT RIGHTS**

1. A partial or full waiver or relaxation of the terms of the Buyer Contract is only valid if it is stated to be a waiver in writing to the other Party.

# **TRANSFERRING RESPONSIBILITIES**

## The Supplier cannot assign, novate or transfer the Buyer Contract or any part of the Buyer Contract without the Buyer's written consent.

## 

## The Buyer can assign, novate or transfer its Buyer Contract or any part of it to any Central Government Body, public or private sector body which performs the functions of the Buyer.

## When the Buyer uses its rights under clause 23.2 the Supplier must enter into a novation agreement in the form that the Buyer specifies.

## The Supplier can terminate the Buyer Contract if it is novated under clause 23.2 to a private sector body that is experiencing an Insolvency Event.

## The Supplier remains responsible for all acts and omissions of the Supplier Staff as if they were its own.

## If the Buyer asks the Supplier for details about subcontractors, the Supplier must provide details of subcontractors at all levels of the supply chain including:

### their name;

### the scope of their appointment; and

### the duration of their appointment.

# 

# **CHANGING THE CONTRACT**

## Either Party can request a variation to the Buyer Contract which is only effective if agreed in writing and signed by both Parties. The Buyer is not required to accept a variation request made by the Supplier.

## For 101(5) of the Regulations, if the Court declares any variation to the Buyer Contract ineffective, the Parties agree that their mutual rights and obligations will be regulated by the terms of the Buyer Contract as they existed immediately prior to that variation and as if the Parties had never entered into that variation.

# **HOW TO COMMUNICATE ABOUT THE CONTRACT**

## All notices under the Buyer Contract must be in writing and are considered effective on the Working Day of delivery as long as they are delivered before 5:00pm on a Working Day. Otherwise the notice is effective on the next Working Day. An email is effective at 9:00am on the first Working Day after sending unless an error message is received.

## Notices to the Buyer or Supplier must be sent to their address in the Letter or in the email of acceptance, respectively.

## This clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

# 

# **PREVENTING FRAUD, BRIBERY AND CORRUPTION**

## The Supplier must not during the Term:

### commit a Prohibited Act or any other criminal offence referred to in Section 2 of the Suitability Assessment Questionnaire; or

### do or allow anything which would cause the Buyer, including any of its employees, consultants, contractors, subcontractors or agents to breach any of the Relevant Requirements or incur any liability under them.

## The Supplier must during the Term:

### create, maintain and enforce adequate policies and procedures to ensure it complies with the Relevant Requirements to prevent a Prohibited Act and require its subcontractors to do the same;

### keep full records to show it has complied with its obligations under clause 26 and give copies to the Buyer on request; and

### if required by the Buyer, within 20 Working Days of the first day of the Term, and then annually, certify in writing to the Buyer, that they have complied with clause 26, including compliance of Supplier Staff, and provide reasonable supporting evidence of this on request, including its policies and procedures.

## The Supplier must immediately notify the Buyer if it becomes aware of any breach of clauses 26.1 or 26.2 or has any reason to think that it, or any of the Supplier Staff, has either:

### been investigated or prosecuted for an alleged Prohibited Act;

### been debarred, suspended, proposed for suspension or debarment, or is otherwise ineligible to take part in procurement programmes or contracts because of a Prohibited Act by any government department or agency;

### received a request or demand for any undue financial or other advantage of any kind related to the Buyer Contract; or

### suspected that any person or Party directly or indirectly related to the Buyer Contract has committed or attempted to commit a Prohibited Act.

## If the Supplier notifies the Buyer as required by clause 26.3, the Supplier must respond promptly to their further enquiries, co-operate with any investigation and allow the audit of any books, records and relevant documentation.

## In any notice the Supplier gives under clause 26.3 it must specify the:

### Prohibited Act;

### identity of the Party who it thinks has committed the Prohibited Act; and

### action it has decided to take.

# **EQUALITY, DIVERSITY AND HUMAN RIGHTS**

## The Supplier must follow all applicable equality law when they perform their obligations under the Buyer Contract, including:

### protections against discrimination on the grounds of race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise; and

### any other requirements and instructions which the Buyer reasonably imposes related to equality Law.

## The Supplier must take all necessary steps, and inform the Buyer of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on the Buyer Contract.

# **HEALTH AND SAFETY**

## The Supplier must perform its obligations meeting the requirements of:

### all applicable Law regarding health and safety; and

### the Buyer's current health and safety policy while at the Buyer’s premises, as provided to the Supplier.

## The Supplier and the Buyer must as soon as possible notify the other of any health and safety incidents or material hazards they are aware of at the Buyer premises that relate to the performance of the Buyer Contract.

# **ENVIRONMENT**

## When working at the Buyer’s premises, the Supplier must perform its obligations under the Buyer's current Environmental Policy, which the Buyer must provide.

## The Supplier must ensure that Supplier Staff are aware of the Buyer's Environmental Policy.

# **TAX**

## The Supplier must not breach any tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines. The Buyer cannot terminate the Buyer Contract where the Supplier has not paid a minor tax or social security contribution.

## 

## Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance contributions in the UK relating to payment received under the Buyer Contract, the Supplier must both:

### comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, the Social Security Contributions and Benefits Act 1992 (including IR35) and National Insurance contributions; and

### indemnify the Buyer against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Term in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff.

## If any of the Supplier Staff are Workers who receive payment relating to the Deliverables, then the Supplier must ensure that its contract with the Worker contains the following requirements:

### the Buyer may, at any time during the Term, request that the Worker provides information which demonstrates they comply with clause 30.2, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding;

### the Worker's contract may be terminated at the Buyer's request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer;

### the Worker's contract may be terminated at the Buyer's request if the Worker provides information which the Buyer considers is not good enough to demonstrate how it complies with clause 30.2 or confirms that the Worker is not complying with those requirements; and

### the Buyer may supply any information they receive from the Worker to HMRC for revenue collection and management.

# 

# **CONFLICT OF INTEREST**

## The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual or potential conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to the Buyer under the Buyer Contract, in the reasonable opinion of the Buyer (a “**Conflict of Interest**”).

## The Supplier must promptly notify and provide details to the Buyer if a Conflict of Interest happens or is expected to happen.

## The Buyer can terminate its Buyer Contract immediately by giving notice in writing to the Supplier or take any steps it thinks are necessary where there is or may be an actual or potential Conflict of Interest.

# **REPORTING A BREACH OF THE CONTRACT**

## As soon as it is aware of it the Supplier and Supplier Staff must report to the Buyer any actual or suspected breach of Law, clause 13 or clauses 26 to 31.

## The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in clause 32.1.

# 

# **RESOLVING DISPUTES**

## If there is a dispute between the Parties, their senior representatives who have authority to settle the dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the dispute.

## If the dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution (CEDR) Model Mediation Procedure current at the time of the dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the dispute, the dispute must be resolved using clauses 33.3 to 33.5.

## 

## Unless the Buyer refers the dispute to arbitration using clause 33.4, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:

### determine the dispute;

### grant interim remedies; and

### grant any other provisional or protective relief.

## 

## The Supplier agrees that the Buyer has the exclusive right to refer any dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

## 

## The Buyer has the right to refer a dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under clause 33.3, unless the Buyer has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under clause 33.4.

## The Supplier cannot suspend the performance of the Buyer Contract during any dispute.

# **WHICH LAW APPLIES**

1. This Buyer Contract and any claim, dispute or difference (whether contractual or non-contractual) arising out of, or connected to it, are governed by English law.

**Annex B**

**Special Terms**

1. **Safeguarding Children and Vulnerable Adults**

|  |  |
| --- | --- |
| “Regulated Activity” | In relation to children as defined in Part 1 of Schedule 4 to the Safeguarding Vulnerable Groups Act 2006.  In relation to vulnerable adults as defined in Part 2 of Schedule 4 to the Safeguarding Vulnerable Groups Act 2006. |

1.1 The Contractor will put in place safeguards to protect children and vulnerable adults from a risk of significant harm which could arise from the performance of this Contract. The Contractor will agree these safeguards with the Department before commencing work on the Contract.

1.2 In addition, the Contractor will carry out checks with the Disclosure and Barring Service (DBS checks) on all staff employed on the Contract in a Regulated Activity. Contractors must have a DBS check done every three years for each relevant member of staff for as long as this Contract applies. The DBS check must be completed before any of the Contractor’s employees work with children in Regulated Activity.

1.3 The Contractor shall immediately notify the Department of any information that it reasonably requests to enable it to be satisfied that the obligations of this Clause 1.1 have been met.

1.4 The Contractor shall not employ or use the services of any person who is barred from, or whose previous conduct or records indicate that he or she would not be suitable to carry out Regulated Activity or who may otherwise present a risk to children or vulnerable adults.

1. **Project outputs**

2.1 Unless otherwise agreed between the Contractor and the Project Manager, all outputs from the Project shall be published by the Department on the Department’s research website.

2.2 The Contractor shall ensure that all outputs for publication by the Department adhere to the Department’s Style Guide and MS Word Template, available to download from:

<https://www.gov.uk/government/publications/research-reports-guide-and-template>.

2.3 Unless otherwise agreed between the Contractor and Project Manager, the Contractor shall supply the Project Manager with a draft for comment at least eight weeks before the intended publication date, for interim reports, and eight weeks before the contracted end date, for final reports.

2.4 The Contractor shall consider revisions to the drafts with the Project Manager in the light of the Department’s comments. The Contractor shall provide final, signed off interim reports and other outputs planned within the lifetime of the Project to the Department by no later than four weeks before the intended publication date, and final, signed off reports and other outputs at the end of the Project to the Department by no later than the contracted end date for the Project.

2.5 Until the date of publication, findings from all Project outputs shall be treated as confidential. The Contractor shall not release findings to the press or disseminate them in any way or at any time prior to publication without approval of the Department.

2.6 Where the Contractor wishes to issue a Press Notice or other publicity material containing findings from the Project, notification of plans, including timing and drafts of planned releases shall be submitted by the Contractor to the Project Manager at least three weeks before the intended date of release and before any agreement is made with press or other external audiences, to allow the Department time to comment. All Press Notices released by the Department or the Contractor shall state the full title of the research report, and include a hyperlink to the Department’s research web pages, and any other web pages as relevant, to access the publication/s. This clause applies at all times prior to publication of the final report.

* 1. Where the Contractor wishes to present findings from the Project in the public domain, for example at conferences, seminars, or in journal articles, the Contractor shall notify the Project Manager before any agreement is made with external audiences, to allow the Department time to consider the request. The Contractor shall only present findings that will already be in the public domain at the time of presentation, unless otherwise agreed with the Department. This clause applies at all times prior to publication of the final report.

1. **Departmental Security Standards for Business Services and ICT Contracts**

In this Schedule, the following words shall have the following meanings and they shall supplement the other definitions in the Contract:

|  |  |
| --- | --- |
| “BPSS”  “Baseline Personnel Security Standard” | the Government’s HMG Baseline Personal Security Standard. Further information can be found at: <https://www.gov.uk/government/publications/government-baseline-personnel-security-standard> |
| “CCSC”  “Certified Cyber Security Consultancy” | is the National Cyber Security Centre’s (NCSC) approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards.  See website:  <https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy> |
| “CCP”  “Certified Professional” | is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession. See website:  <https://www.ncsc.gov.uk/information/about-certified-professional-scheme> |
| “Cyber Essentials”  “Cyber Essentials Plus” | Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme.  There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to these providers:  <https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body> |
| “Data”  “Data Controller”  “Data Protection Officer”  “Data Processor”  “Personal Data”  “Personal Data requiring Sensitive  Processing”  “Data Subject”, “Process” and “Processing” | shall have the meanings given to those terms by the Data Protection Legislation |
| "Buyer’s Data"  “Buyer’s Information” | is any data or information owned or retained to meet departmental business objectives and tasks, including:  (a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are:  (i) supplied to the Supplier by or on behalf of the Buyer; or  (ii) which the Supplier is required to generate, process, store or transmit pursuant to this Contract; or  (b) any Personal Data for which the Buyer is the Data Controller; |
| “Departmental Security Requirements” | the Buyer’s security policy or any standards, procedures, process or specification for security that the Supplier is required to deliver. |
| “Digital Marketplace / G-Cloud” | the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects. |
| “End User Devices” | the personal computer or consumer devices that store or process information. |
| “Good Industry Standard”  “Industry Good Standard” | the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector. |
| “GSC”  “GSCP” | the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: <https://www.gov.uk/government/publications/government-security-classifications> |
| “HMG” | Her Majesty’s Government |
| “ICT” | Information and Communications Technology (ICT) and is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution |
| “ISO/IEC 27001” “ISO 27001” | is the International Standard for Information Security Management Systems Requirements |
| “ISO/IEC 27002” “ISO 27002” | is the International Standard describing the Code of Practice for Information Security Controls. |
| “ISO 22301” | is the International Standard describing for Business Continuity |
| “IT Security Health Check (ITSHC)”  “IT Health Check (ITHC)”  “Penetration Testing” | an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that ICT system. |
| “Need-to-Know” | the Need-to-Know principle employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties. |
| “NCSC” | the National Cyber Security Centre (NCSC) is the UK government’s National Technical Authority for Information Assurance. The NCSC website is <https://www.ncsc.gov.uk> |
| “OFFICIAL”  “OFFICIAL-SENSITIVE” | the term ‘OFFICIAL’ is used to describe the baseline level of ‘security classification’ described within the Government Security Classification Policy (GSCP).    the term ‘OFFICIAL–SENSITIVE is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the GSCP. |
| “RBAC”  “Role Based Access Control” | Role Based Access Control, a method of restricting a person’s or process’ access to information depending on the role or functions assigned to them. |
| “Storage Area Network”  “SAN” | an information storage system typically presenting block based storage (i.e. disks or virtual disks) over a network interface rather than using physically connected storage. |
| “Secure Sanitisation” | the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level.  NCSC Guidance can be found at: <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>  The disposal of physical documents and hardcopy materials advice can be found at: <https://www.cpni.gov.uk/secure-destruction-0> |
| “Security and Information Risk Advisor”  “CCP SIRA”  “SIRA” | the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also:  <https://www.ncsc.gov.uk/articles/about-certified-professional-scheme> |
| “Senior Information Risk Owner”  “SIRO” | the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for overseeing the management of information risk across the organisation. This includes its executive agencies, arm’s length bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties. |
| “SPF”  “HMG Security Policy Framework” | the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government’s Official Committee on Security on how HMG organisations and third parties handling HMG information and other classification will apply protective security to ensure HMG can function effectively, efficiently and securely. <https://www.gov.uk/government/publications/security-policy-framework> |
| "Supplier Staff" | all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier’s obligations under the Contract. |

* 1. The Supplier shall be aware of and comply with the relevant [HMG security policy framework](https://www.gov.uk/government/publications/security-policy-framework), [NCSC guidelines](https://www.ncsc.gov.uk/section/advice-guidance/all-topics) and where applicable these Departmental Security Requirements which include but are not constrained to the following paragraphs.
  2. Where the Supplier will provide products or Services or otherwise handle information at OFFICIAL for the Buyer, the requirements of [Procurement Policy Note: Updates to the Cyber Essentials Scheme (PDF)](https://assets.publishing.service.gov.uk/media/652d2b6ad86b1b000d3a4fbe/2023-10-11_Updated_PPN_09_23_Cyber_Essentials_eg.pdf) - Action Note 09/23 dated September 2023, or any subsequent updated document, are mandated, namely that contractors supplying products or services to HMG shall have achieved and will retain Cyber Essentials certification at the appropriate level for the duration of the contract. The certification scope shall be relevant to the Services supplied to, or on behalf of, the Buyer.
  3. Where paragraph 3.2 above has not been met, the Supplier shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements). The ISO/IEC 27001 certification must have a scope relevant to the Services supplied to, or on behalf of, the Buyer. The scope of certification and the statement of applicability must be acceptable, following review, to the Buyer, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).
  4. The Supplier shall follow the UK Government Security Classification Policy (GSCP) in respect of any Buyer’s Data being handled in the course of providing the Services and will handle all data in accordance with its security classification. (In the event where the Supplier has an existing Protective Marking Scheme then the Supplier may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Buyer’s Data).
  5. Buyer’s Data being handled while providing an ICT solution or service must be separated from all other data on the Supplier’s or sub-contractor’s own IT equipment to protect the Buyer’s Data and enable the data to be identified and securely deleted when required in line with paragraph 3.14. For information stored digitally, this must be at a minimum logically separated. Physical information (e.g., paper) must be physically separated.
  6. The Supplier shall have in place and maintain physical security to premises and sensitive areas used in relation to the delivery of the products or Services, and that store or process Buyer’s Data, in line with ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access), CCTV, alarm systems, etc.   
       
     3.6.1. Where remote working is allowed, the Supplier shall have an appropriate remote working policy in place for any Supplier staff that will have access to the Buyer’s data and/or systems.
  7. The Supplier shall have in place, implement and maintain an appropriate user access control policy for all ICT systems to ensure only authorised personnel have access to Buyer’s Data. This policy should include appropriate segregation of duties and if applicable role based access controls (RBAC). User credentials that give access to Buyer’s Data or systems shall be considered to be sensitive data and must be protected accordingly.
  8. The Supplier shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Buyer’s Data, including but not limited to:
     1. physical security controls;
     2. good industry standard policies and processes;
     3. malware protection;
     4. boundary access controls including firewalls, application gateways, etc;
     5. maintenance and use of fully supported software packages in accordance with vendor recommendations;
     6. use of secure device configuration and builds;
     7. software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;
     8. user identity and access controls, including the use of multi-factor authentication for sensitive data and privileged account accesses;
     9. any services provided to the Buyer must capture audit logs for security events in an electronic format at the application, service and system level to meet the Buyer’s logging and auditing requirements, plus logs shall be:
        1. retained and protected from tampering for a minimum period of six months;
        2. made available to the Buyer on request.
  9. The Supplier shall ensure that any Buyer’s Data (including email) transmitted over any public network (including the Internet, mobile networks or unprotected enterprise network) or to a mobile device shall be encrypted when transmitted.
  10. The Supplier shall ensure that any Buyer’s Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Buyer except where the Buyer has given its prior written consent to an alternative arrangement.
  11. The Supplier shall ensure that any device which is used to process Buyer’s Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/end-user-device-security> and <https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles>.
  12. Whilst in the Supplier’s care all removable media and hardcopy paper documents containing Buyer’s Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.

The term ‘lock and key’ is defined as: “securing information in a lockable desk drawer, cupboard or filing cabinet which is under the user’s sole control and to which they hold the keys”.

* 1. When necessary to hand carry removable media and/or hardcopy paper documents containing Buyer’s Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This paragraph shall apply equally regardless of whether the material is being carried inside or outside of company premises.

The term ‘under cover’ means that the information is carried within an opaque folder or envelope within official premises and buildings and within a closed briefcase or other similar bag or container when outside official premises or buildings.

* 1. In the event of termination of Contract due to expiry, as a result of an Insolvency Event or for breach by the Supplier, all information assets provided, created or resulting from provision of the Services shall not be considered as the Supplier’s assets and must be returned to the Buyer and written assurance obtained from an appropriate officer of the Supplier that these assets regardless of location and format have been fully sanitised throughout the Supplier’s organisation in line with paragraph 3.15.
  2. In the event of termination, equipment failure or obsolescence, all Buyer’s Data and Buyer’s Information, in either hardcopy or electronic format, that is physically held or logically stored by the Supplier must be accounted for and either physically returned or securely sanitised or destroyed in accordance with the current HMG policy using an NCSC-approved product or method.

Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as data stored in a cloud system, Storage Area Network (SAN) or on shared backup tapes, then the Supplier shall protect (and ensure that any sub-contractor protects) the Buyer’s Information and Buyer’s Data until such time, which may be long after termination or expiry of the Contract, when it can be securely cleansed or destroyed.

Evidence of secure destruction will be required in all cases.

* 1. Access by Supplier Staff to Buyer’s Data, including user credentials, shall be confined to those individuals who have a “need-to-know” in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Buyer. All Supplier Staff must complete this process before access to Buyer’s Data is permitted. [Any Supplier Staff who will be in contact with children or vulnerable adults must, in addition to any security clearance, have successfully undergone an Enhanced DBS (Disclosure and Barring Service) check prior to any contact].
  2. All Supplier Staff who handle Buyer’s Data shall have annual awareness training in protecting information.
  3. Notwithstanding any other provisions as to business continuity and disaster recovery in the Contract, the Supplier shall, as a minimum, have in place robust business continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the Contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the Services delivered. If an ISO 22301 certificate is not available the supplier will provide evidence of the effectiveness of their ISO 22301 conformant business continuity arrangements and processes including IT disaster recovery plans and procedures. This must include evidence that the Supplier has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.
  4. Any suspected or actual breach of the confidentiality, integrity or availability of Buyer’s Data, including user credentials, used or handled while providing the Services shall be recorded as a Security Incident. This includes any non-compliance with the Departmental Security Requirements and these provisions, or other security standards pertaining to the solution.

Security Incidents shall be reported to the Buyer immediately, wherever practical, even if unconfirmed or when full details are not known, but always within 24 hours of discovery. If Security Incident reporting has been delayed by more than 24 hours, the Supplier should provide an explanation about the delay.

Security Incidents shall be reported through the Buyer’s nominated system or service owner.

Security Incidents shall be investigated by the Supplier with outcomes being notified to the Buyer.

* 1. The Supplier shall ensure that any Supplier ICT systems and hosting environments that are used to handle, store or process Buyer’s Data, including Supplier ICT connected to Supplier ICT systems used to handle, store or process Buyer’s Data, shall be subject to independent IT Health Checks (ITHC) using an NCSC CHECK Scheme ITHC provider before go-live and periodically (at least annually) thereafter. On request by the Buyer, the findings of the ITHC relevant to the Services being provided are to be shared with the Buyer in full without modification or redaction and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required, to be determined by the Buyer upon review of the ITHC findings.
  2. The Supplier or sub-contractors providing the Services will provide the Buyer with full details of any actual or future intent to develop, manage, support, process or store Buyer’s Data outside of the UK mainland. The Supplier or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Buyer.
  3. The Buyer reserves the right to audit the Supplier or sub-contractors providing the Services annually, within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the Services being supplied and the Supplier’s, and any sub-contractors’, compliance with the paragraphs contained in this Schedule.
  4. The Supplier and sub-contractors shall undergo appropriate security assurance activities and shall provide appropriate evidence including the production of the necessary security documentation as determined by the Buyer through the life of the contract. This will include obtaining any necessary professional security resources required to support the Supplier’s and sub-contractor’s security assurance activities such as: a Security and Information Risk Advisor (SIRA) certified to NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Cyber Professional (CCP) schemes.
  5. Where the Supplier is delivering an ICT solution to the Buyer they shall design and deliver solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current NCSC Information Assurance Guidance and Buyer’s Policy. The Supplier will provide the Buyer with evidence of compliance for the solutions and services to be delivered. The Buyer’s expectation is that the Supplier shall provide written evidence of:
     1. Implementation of the foundational set of cyber defence safeguards from the Center for Internet Security Critical Security Controls (CIS CSC v8).
     2. any existing security assurance for the Services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification issued by the United Kingdom Accreditation Service.
     3. any existing HMG security accreditations or assurance that are still valid including: details of the awarding body; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement.
     4. documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Supplier shall provide details of who the awarding body or organisation will be, and date expected.
     5. compliance with the principles of secure by Design as described at [Secure by Design Principles - UK Government Security](https://www.security.gov.uk/guidance/secure-by-design/principles/).

Additional information and evidence to that listed above may be required to ensure compliance with DfE security requirements as part of the DfE security assurance process. Where a request for evidence or information is made by the Buyer, the Supplier will acknowledge the request within 5 working days and either provide the information within that timeframe, or, if that is not possible, provide a date when the information will be provided to the Buyer. In any case, the Supplier must respond to information requests from the Buyer needed to support the security assurance process promptly and without undue delay.

* 1. The Supplier shall contractually enforce all these Departmental Security Requirements onto any third-party suppliers, sub-contractors or partners who will have access to the Buyer’s Data in the course of providing the Services, before access to the data is provided or permitted.
  2. The Supplier shall comply with the [NCSC’s social media guidance: how to use social media safely](https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely) for any web and social media-based communications. In addition, any Communications Plan deliverable must include a risk assessment relating to the use of web and social media channels for the programme, including controls and mitigations to be applied and how the NCSC social media guidance will be complied with. The Supplier shall implement the necessary controls and mitigations within the plan and regularly review and update the risk assessment throughout the contract period. The Buyer shall have the right to review the risks within the plan and approve the controls and mitigations to be implemented, including requiring the Supplier to implement any additional reasonable controls to ensure risks are managed within the Buyer’s risk appetite.
  3. Any Supplier ICT system used to handle, store or process the Buyer’s Data, including any Supplier ICT systems connected to systems that handle, store or process the Buyer’s Data, must have in place protective monitoring at a level that is commensurate with the security risks posed to those systems and the data held. The Supplier shall provide evidence to the Buyer upon request of the protective monitoring arrangements in place needed to assess compliance with this requirement.
  4. Where the Supplier is using Artificial Intelligence (AI) and/or Machine Learning (ML) in the delivery of their service to the Buyer, this shall comply with the NCSC’s [principles for the security of machine learning](https://www.ncsc.gov.uk/collection/machine-learning).

1. **Indexation**
   1. Any amounts or sums in this Agreement which are expressed to be “subject to Indexation” shall be adjusted in accordance with the provisions of this Paragraph 4 to reflect the effects of inflation.
   2. Where Indexation applies, the relevant adjustment shall be:

(a) applied on the first day of the second April following the Effective Date and on the first day of April in each subsequent year (each such date an “adjustment date”); and

(b) determined by multiplying the relevant amount or sum by the percentage increase or changes in the [Consumer Price Index] published for the 12 months ended on the 31 January immediately preceding the relevant adjustment date.

* 1. Except as set out in this Paragraph 4, neither the Charges nor any other costs, expenses, fees or charges shall be adjusted to take account of any inflation, change to exchange rate, change to interest rate or any other factor or element which might otherwise increase the cost to the Supplier or Sub-contractors of the performance of their obligations.

**Annex C**

**Contract Management Information**

PAYMENT

PAYMENT METHOD

Via BACS upon submission of valid invoice

BUYER’S INVOICE ADDRESS:

Department for Education, Sanctuary Buildings, Great Smith Street,

London SW1P 3BT

Invoices must be submitted in pdf format, state the Purchase Order number (provided separately to this form), and sent via email to [AccountsPayable.OCR@education.gov.uk](mailto:Accounts.PayableOCR@education.gov.uk)

PROCEDURES AND POLICIES

BUYER’S ENVIRONMENTAL POLICY

Department for Education Sustainability and Climate Change Strategy, 21 April 2022,available online at: [Sustainability and climate change strategy - GOV.UK](https://www.gov.uk/government/publications/sustainability-and-climate-change-strategy)

BUYER’S SECURITY POLICY

Department for Education Personal Information Charter, available online at: <https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter#co>

The Buyer may require the Supplier to ensure that any person employed in the delivery of the Deliverables has undertaken a Disclosure and Barring Service check.

The Supplier shall ensure that no person who discloses that he/she has a conviction that is relevant to the nature of the Buyer Contract, relevant to the work of the Buyer, or is of a type otherwise advised by the Buyer (each such conviction a "**Relevant Conviction**"), or is found by the Supplier to have a Relevant Conviction (whether as a result of a police check, a Disclosure and Barring Service check or otherwise) is employed or engaged in the provision of any part of the Deliverables.

MAXIMUM LIABILITY AMOUNT

**Liability cap which applies in respect of all liabilities under the Buyer Contract:** £190,000

**Annex D**

**Processing Data**

**Status of the Controller**

* 1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under the Buyer Contract dictates the status of each party under the Data Protection Act 2018. A Party may act as:
     1. “Controller” in respect of the other Party who is “Processor”;
     2. “Processor” in respect of the other Party who is “Controller”;
     3. “Joint Controller” with the other Party;
     4. “Independent Controller” of the Personal Data where the other Party is also “Controller”,

in respect of certain Personal Data under a Buyer Contract and shall specify in Appendix 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

**Where one Party is Controller and the other Party its Processor**

* 1. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Appendix 1 *(Processing Personal Data*) by the Controller.
  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:
     1. a systematic description of the envisaged Processing and the purpose of the Processing;
     2. an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
     3. an assessment of the risks to the rights and freedoms of Data Subjects; and
     4. 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 the Buyer Contract:
     1. Process that Personal Data only in accordance with Appendix 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
     2. ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in clause 14.3 of the Conditions*,* which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:
        1. nature of the data to be protected;
        2. harm that might result from a Personal Data Breach;
        3. state of technological development; and
        4. cost of implementing any measures;
     3. ensure that :
        1. the Processor Personnel do not Process Personal Data except in accordance with the Buyer Contract (and in particular Appendix 1 *(Processing Personal Data*));
        2. 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:
           1. are aware of and comply with the Processor’s duties under this Annex D, clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Conditions;
           2. are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
           3. 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 the Buyer Contract; and
           4. have undergone adequate training in the use, care, protection and handling of Personal Data;
     4. not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
        1. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;
        2. the Data Subject has enforceable rights and effective legal remedies;
        3. 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
        4. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and
     5. at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Buyer Contract unless the Processor is required by Law to retain the Personal Data.
  5. Subject to paragraph 7 of this Annex D, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Buyer Contract it:
     1. receives a Data Subject Access Request (or purported Data Subject Access Request);
     2. receives a request to rectify, block or erase any Personal Data;
     3. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
     4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Buyer Contract;
     5. 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
     6. becomes aware of a Personal Data Breach.
  6. The Processor’s obligation to notify under paragraph 6 of this Annex D 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 assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Annex D (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
     1. the Controller with full details and copies of the complaint, communication or request;
     2. such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
     3. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
     4. assistance as requested by the Controller following any Personal Data Breach; and/or
     5. 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 Annex D. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
     1. the Controller determines that the Processing is not occasional;
     2. 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
     3. 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. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
  11. Before allowing any Subprocessor to Process any Personal Data related to the Buyer Contract, the Processor must:
      1. notify the Controller in writing of the intended Subprocessor and Processing;
      2. obtain the written consent of the Controller;
      3. enter into a written agreement with the Subprocessor which give effect to the terms set out in this Annex D such that they apply to the Subprocessor; and
      4. provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
  12. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
  13. The Buyer may, at any time on not less than thirty (30) Working Days’ notice, revise this Annex D 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 the Buyer Contract).
  14. The Parties agree to take account of any guidance issued by the Information Commissioner’s Office. The Buyer may on not less than thirty (30) Working Days’ notice to the Supplier amend the Buyer Contract to ensure that it complies with any guidance issued by the Information Commissioner’s Office.

**Where the Parties are Joint Controllers of Personal Data**

* 1. In the event that the Parties are Joint Controllers in respect of Personal Data under the Buyer Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Appendix 2 to this Annex D.

**Independent Controllers of Personal Data**

* 1. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
  2. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
  3. Where a Party has provided Personal Data to the other Party in accordance with paragraph 7 of this Annex D above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
  4. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Buyer Contract.
  5. The Parties shall only provide Personal Data to each other:
     1. to the extent necessary to perform their respective obligations under the Buyer Contract;
     2. in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and
     3. where it has recorded it in Appendix 1 *(Processing Personal Data).*
  6. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.
  7. A Party Processing Personal Data for the purposes of the Buyer Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.
  8. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Buyer Contract **(“Request Recipient”)**:
     1. the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
     2. where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
        1. promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
        2. provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
  9. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Buyer Contract and shall:
     1. do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
     2. implement any measures necessary to restore the security of any compromised Personal Data;
     3. work with the other Party to make any required notifications to the Information Commissioner’s Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
     4. not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.
  10. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Buyer Contract as specified in Appendix 1 *(Processing Personal Data).*
  11. Personal Data shall not be retained or processed for longer than is necessary to perform each Party’s respective obligations under the Buyer Contract which is specified in Appendix 1 *(Processing Personal Data)*.
  12. Notwithstanding the general application of paragraphs 2 to 15 of this Annex D to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 17 to 27 of this Annex D.

## **Appendix 1 - Processing Personal Data**

This Appendix shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Appendix shall be with the Buyer at its absolute discretion.

1. The contact details of the Buyer’s Data Protection Officer are: Emma Wharram, Department for Education, 7&8 Wellington Place, Wellington Street, Leeds, LS14AW,

[dataprotection.office@education.gov.uk](mailto:dataprotection.office@education.gov.uk)

1. The contact details of the Supplier’s Data Protection Officer are: redacted, CooperGibson Research,
2. The Processor shall comply with any further written instructions with respect to Processing by the Controller.
3. Any such further instructions shall be incorporated into this Appendix.

|  |  |
| --- | --- |
| **Description** | **Details** |
| Identity of Controller for each Category of Personal Data | **The Buyer is Controller and the Supplier is Processor**  The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 of Annex D and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:  DfE Longitudinal Educational Outcomes Dataset  The LEO dataset will be used to track the employment outcomes of two cohort participating in the Supported Internships programme. Outcomes will be compared to a matched comparison group not participating in the programme.  The following personal data will be collected:  o Individual Learner Record Number  o Gender  o Ethnicity  o Health/Disability Data  o Local Authority Region  o Educational Attainment  Online Survey with young people (pre, post, follow-up and additional yr 1 and yr 2 follow-up)  The supplier will conduct an online survey with young people participating in the SI programme. The following personal data will be collected:  o Name  o Contact details (email, phone number)  o Gender  o Age  o Ethnicity  o Data concerning health and disability  o Technical Device Information- Cookies  o Internship Information- Job Title, Job Description  o Name of education provider  o Opinions  Online Survey with job coaches  The supplier will conduct an online survey with job coaches working on the SI programme. The following personal data will be collected.  o Contact Details (Name, Email, Telephone)  o Additional role(s)  o Employment contract details  o Local Authority Region  o Employment Information- Length in Post, nature of role  o Opinions  Online Survey with providers  The supplier will conduct an online survey with job coaches working on the SI programme. The following personal data will be collected.  o Contact Details (Name, Email, Telephone)  o Provider information e.g type of provider (school, college etc)  o Funding information  o Additional role(s)  o Local Authority Region  o Opinions  Case Studies  The supplier will conduct case studies with a range of stakeholders, including education providers, supported interns, families, local authority representative, job coaches and employers. The following personal data will be collected:  o Name  o Contact Details (Email, Telephone, address of employer/education provider)  o Opinions  o Age  o Gender  o Health/Disability Information  o Internship Information (Job Title, Job Description, sector)  o Local Authority/Region.  Placement Visits  The supplier will conduct a series of placement visits. The following personal data will be collected:  o Name of intern  o Contact Details (Email, Telephone)  o Age  o Health/Disability Data o Internship Information (Job Title, Job Description)  o Employer Information (Size, Sector)  o Employer contact details (name, telephone, address)  o Opinions  Focus groups (online)  The supplier will conduct focus groups online with pilot providers and local authority leads. The following personal data will be collected:  o Name  o Contact Details (Email, Telephone, address of LA/education provider)  o Opinions  o Age  o Gender  o Health/Disability Information  o Internship Information (Job Title, Job Description, sector)  o Local Authority/Region.  o Opinions  Monitoring Data  The supplier will receive monitoring data from the policy delivery partner. Monitoring data will include data on:  o Number and types of interns and employers  o Time spent in placement.  o Details of employers and providers  o Number of interns achieving paid employment/outcomes at the end of six months  o Number of providers completing the SI Quality Assurance Framework. |
| Duration of the Processing | Processing will take place for the length of the contract to March 2027. |
| Nature and purposes of the Processing | This data processing will rely on the public task condition, as the processing is necessary for the controller to perform a task in the public interest or for the organisation’s official functions, and the task has a clear basis is law. The processing of personal data is necessary to conduct the evaluation of the pilot extension of the Supported Internships programme. It is in the public interest such that it will provide vital evidence to ensure DfE are funding policy that maximises outcomes for young people with SEND.  The controller needs to process personal data to contact the various stakeholders about the research and invite them to participate. Demographic data is needed to ensure we are building a representative sample and to conduct subgroup analysis i.e. understand if different groups have different experiences/outcomes on the SI programme. |
| Type of Personal Data | *See above.* |
| Categories of Data Subject | The following groups will be participating:  o Young people participating in the SI evaluation  o Employers participating in the SI evaluation  o Education Providers  o Families  o Job Coaches  o Local Authority Representatives |
| 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 | Data will be retained for the length of the contract, to March 2027 and shall be destroyed upon contract cessation. The data processor shall only hold data for the processing period. At the completion of this processing period, the data processor shall delete the data held. The Department shall hold the data for as long as there is needed for this data, as per the lawful basis of legitimate interest. |

**Annex F**

**Part 1 – Deliverables**

The one-year extension of the pilot supported internships programme is to be evaluated against the following three aims.

Aim 1: Assess how, and to what extent, the SR policy investment led to an increase in the quantity of non-EHCP pilot SI placements.

Aim 2: Determine how, and to what extent, supported internships improve feelings of readiness for work for the non-EHCP pilot cohort.

Aim 3: Determine to what extent the supported internships model works for the pilot cohort for those involved in running and providing the provision.

The activity involved in the evaluation is outlined below.

|  |  |  |
| --- | --- | --- |
| **PROJECT STAGE** | **ACTIVITY** | **NOTES** |
| PROJECT MANAGEMENT | Project management and admin, liaison with DfE and updates | Weekly updates and meetings for 1 year for 3 supplier staff and general project management and admin. |
| Liaison with delivery partners and updates | Monthly meet/minutes. |
| Internal meetings and briefings |  |
|  |  |  |
| DESIGN | Liaison with LAs and providers, collating & updating sample details - continuous liaison re timings, recruitment | Rolling starts/ends means continuous liaison required. Will need to liaise throughout re recruitment/onboarding, timings, collating sample details, maintaining contact for longitudinal aspects. |
| Review ethical approvals |  |
| Review Theory of Change to account for the pilot delivery extension | Review from quant, qual, cost and overall evaluation leads. |
| Review intern baseline, endline, follow-up surveys, revisions and testing, provider/intern invites and reminders, privacy policy | 5 surveys, longitudinal FU surveys likely to need new design. |
| Review/revise Job Coach survey and comms/reminders, set-up in software, testing | Significant changes required as aims are different. |
| Design provider survey and comms/reminders, set-up in software, testing |  |
| Review/revise case study materials (inc consents, Topic Guides, invites, info sheets) | Considerable number of documents to amend to ensure relevant to the Yr 3 Pilot - initial invite, invites/info sheets/privacy notice/consent/topic guides & accompanying materials for all stakeholders as previous (interns, employers, providers, parents, LA, JC, graduate interns, non SI yp, placement visit). |
| Design TGs, comms, consents for follow-up interviews with interns, employers, providers for Yr1/2 Pilots | Design for 9 month FU with providers, employers, interns, parents of Yr1/2 cohorts - info materials, consents, TGs, invites. |
| Managing requirements from ONS SRS to access ILR data |  |
| Design comms, materials, TG for Pilot provider/LA focus group |  |
|  |  |  |
| DATA COLLECTION | Liaison with DPs for Pilot Yr 3 MI, collation/recording, review of surveys | Continuous liaison required. |
| Pilot Yr 3 intern pre, post, FU (4 months) surveys | Running 3 surveys, monitoring and amending sample details, dealing with provider queries, comms with sector, monitoring response, reminders and amending & personalising reminders each round. |
| Additional 6 month follow-up survey with pilot intern Yr1 and Yr 2 to track employment outcomes | To include liaison with providers / LA leads / job coaches. |
| JC survey and comms (Pilot Yr 3) | Launch, monitoring, amending sample, reminders. |
| Provider survey & comms (Pilot Yr 3) | Launch, monitoring, amending sample, reminders. |
| Organise and conduct 3 case studies and placement visits of non-EHCP pilot group in pilot Yr 3. To include providers, employers, job coaches, LA, interns and parent/carers. | 3 case study/placement visits conducted. Includes time for organising plus transcription/notes and significant follow-up to collate additional data as required and complete any remaining telephone /online interviews. |
| Organise and conduct phone/Teams interviews with provider, employer (up to 2 if intern moved) & 1 intern from 2 Pilot case studies in Yr 1 or 2 AY23/24 or 24/25 (touch base to see progress / reflect on how it went and outcomes). | Up to 5 interviews per pilot case study. |
| Organise and conduct 2 online focus groups. One for Local Authority leads and one for Pilot providers. | Organising, transcription/notes, min 2 staff attending. |
|  |  |  |
|  | Analysis of Pilot Yr 3 MI and comparison with Pilot Yr1/2 data where available | Data analysis of DP survey/feedback forms (e.g. 2 JC training surveys, engagement forum surveys, LA baseline and follow-up surveys - all with qualitative data). |
| Analysis of Pilot Yr 3 ILR and comparison with Pilot Yr1/2 data where available | Cleaning and managing the data to get it to a suitable place for analysis. Running tables, checking and amending for statistical disclosure control where counts are low. Working with the pilot flag in the ILR. |
| Running tables, checking, analysis of intern pre/post/FU survey+2 additional FU (comparisons to Y1/2) | Includes running and checking, revisions to tables across 5 surveys then analysis. |
| Running tables, checking, analysis of JC/provider surveys (comparisons where possible) | Includes running and checking, revisions to tables across 5 surveys then analysis. |
| Coding/analysis 3 case study data and FU interview data (10 ints/2 pilots) | 3 days per case study to cover coding of qualitative data plus 2 days for analysis+ 2 days for the longitudinal interviews, min 2 days for QA and review. |
| Coding/analysis of 2 provider/LA focus groups | Coding transcripts, analysis and merging with wider data. |
|  |  |  |
| REPORTS/ OUTPUTS | Draft report of Pilot Yr 3, inc revised TOC + 1 additional written case study | Bringing all data together, internal reviews and QA.  Report to include all data on pilot year 3 in full (quantitative and qualitative), and to include pilot years 1 and 2 where follow up activity has been conducted such as the additional follow-up survey for years 1 and 2  and the 2x case studies included in the deliverables.  Quantitative data to be compared in the report to pilot years 1 &2 (without recoding) where possible. For example, comparing quantitative results from the February 2026 report with pilot year 3. |
| Final report and slide deck, meeting | Revisions and finalising report, PPT slides and presentation (3 staff). |
| Accessible summary | Accessible summary report. |
| Transfer of data | Anonymised quantitative data to be transferred to DfE on end of contract. |

**Part 2 – Charges**

**Costing milestones – Evaluation of the supported internships pilot extension**

|  |  |  |
| --- | --- | --- |
| **Milestone** | **Activities** | **Payment** |
| 05/09/2025 | * Research materials revision drafted for the pilot year 3 extension. * Ethical approval application. * Liaison with LAs and providers to collate sample details. | redacted |
| 05/12/2025 | * Pilot year 3 intern baseline survey complete. * Additional follow-up survey with year 1 pilot interns complete. * Analysis of the baseline survey and follow-up year 1 survey (data checking / cleaning and production of tables). | redacted |
|  | **FY25/26** | redacted |
| 01/09/2026 | * Pilot year 3 intern post survey complete and analysed (data checking / cleaning and production of tables). * Pilot year 3 job coach and provider survey complete. * 2 x Online focus groups, one with pilot providers and one with pilot LAs complete. * 2 x Pilot year 1 or year 2 case study online / phone follow up complete. * 3 x Pilot year 3 case studies and placement visits complete. | redacted |
| 19/12/2026 | * Pilot year 3 job coach and provider surveys analysed (data checking / cleaning and production of tables). * Pilot online focus groups with providers and LAs analysed. * Online focus groups (x2), pilot year 1 or 2 case studies (2) and pilot year 3 case studies and placement visits (3) analysed. * Pilot year 3 intern follow-up survey launched. * Follow-up survey with year 2 pilot interns launched. | redacted |
| 01/03/2027 | * Analysis complete of pilot year 3 intern follow up survey (data checking / cleaning and production of tables). * Analysis complete of follow-up survey with year 2 pilot interns (data checking / cleaning and production of tables). * Draft report including analysis of all listed research methods, case studies and PowerPoint presentation shared with DfE. * Final report signed-off by DfE. * Accessible summary signed off by DfE. * Transfer of anonymised survey data collected in the evaluation to DfE. | redacted |
|  | **FY26/27** | redacted |
|  | **Project Total** | redacted |