Clause Page

CONTENTS

DATE

PARTIES

(1) [O] [(No.[O] / trading together in partnership under the style [O] / a limited liability partnership] [whose registered Office is [o] / whose principal place Of business is ['Il (Sub-Consultant),

(2) [o] [(No.(•] / trading together in partnership under the style ['J I a limited liability partnership] [whose registered office is [O] / whose principal place of business is (Beneficiary).

(3) [O] [(No.[O] / trading together in partnership under the style [O] I a limited liability partnership] [whose registered office is [o] / whose principal place of business is (Consultant).

BACKGROUND

(A) By the Appointment, [o] [(Nom[O] / trading together in partnership under the style [o] / a limited liability partnership] [whose registered office is [e] / whose principal place of business is [●]] (Employer) has engaged the Consultant to act in the capacity of [o] in relation to the [design, specification, construction and completion of the Development at the Site] on the terms and subject to the conditions set out in the Appointment.

(B) By the Contract, the Consultant has employed the Sub-Consultant to carry out various services, duties and obligations on the terms and subject to the conditions set out in the Contract.

(C) The Beneficiary has entered into an agreement [to purchase I for lease to take a lease of / to provide finance forl [the whole of / part of] the [Development / Site].

(D) The Sub-Consultant has agreed to enter into this Deed for the benefit of the Beneficiary and its successors in title and assigns.

AGREED TERMS

In consideration of the payment of El by the Beneficiary to the Sub-Consultant (receipt of which is hereby acknowledged) and which the parties hereby agree to be full and valuable consideration it is hereby agreed that:

1.DEFINITIONS AND INTERPRETATION

1.1In this Deed the words below have the meanings next to them unless the context requires otherwise:

Appointment	the JCT Consultancy Agreement 2016 (as amended) entered into between the Employer and the Consultant dated [O] for the carrying out of services, duties and obligations in relation to the Development including any documents or arrangements which are supplemental or ancillary to it by way of variation or otherwise,
Business Day	a day which is not a Saturday or Sunday or a bank or national holiday in England
Construction Products Regulations	UK Construction Products Regulation 201 1 and the Construction Products Regulations 2013 (Sl 2013/1387).
Contract	the contract between the Consultant and the Sub-Consultant dated [o] for the carrying out Of various services, duties and obligations in relation to the Development including any documents or arrangements which are supplemental or ancillary to it by way of variation or otherwise,

Development	the development of [O] by the Employer at the Site.
Group	in relation to a company: (a) that company and any Subsidiary of that company; (b) the ultimate Holding Company of that company, and (c) every other company which is a Subsidiary of the same ultimate Holding Company, in each case from time to time.
Group Company	in relation to a Group any member of that Group.
Holding Company	has the meaning given to that term in section 1 159 Companies Act 2006 and a company will be treated, for the purposes only of the membership requirement contained in sub-sections 1 159(1)(b) and (c), as a member of another company even if its shares in that other company are registered in the name of (a) a person (or its nominee) whether by way of security or in connection with the taking of security or (b) its nominee.
Material	all designs, drawings, calculations, charts, diagrams, sketchest models, plans, specifications, design details, photographs, brochures, reports, notes of meetings, CAD materials, data, databases, schedules, programmes, bills of quantities, budgets, surveys, levels, setting out dimensions and/or all other documents or materials produced or prepared by or on behalf of the SubConsultant in relation to and/or connection with the Development and/or Site (including any and all updates, amendments, additions and revisions to them and any works, designs or inventions contained incorporated or referred to in them for any purpose relating to the Development and/or Site) created before, on or after the date Of this Deed,
Practical Completion	the date of practical completion of the Development as certified or otherwise evidenced as required under the terms of the relevant building contract,
Site	the land at (o] upon which the Development is to be constructed.
Subsidiary	has the meaning given to that term in section 1 159 Companies Act 2006 and a company will be treated, for the purposes only of the membership requirement contained in sub-sections 1 159(1)(b) and (c), as a member of another company even if its shares in that other company are registered in the name of (a) a person (or its nominee) whether by way of secu rity or in connection with the taking of security or (b) its nominee.

UK Construction Products the UK version of Regulation (EU) No 305/201 1 , as it forms part of Regulation 2011 English law under the European Union (Withdrawal) Act 2018.

€2 In this Deed unless the context requires otherwise.

12.1 references to a Clause or Schedule are to a clause of, or schedule to this Deed, references to this Deed include its schedules, and references in a Schedule to a paragraph are to a paragraph of that Schedule;

2.2 references to this Deed or any other document are to this Deed or that document as amended or novated from time to time;

1 .2.3 words denoting the singular include the plural and vice versa;

1.24 references to a person include any corporate or unincorporated body;

1 .2.5 the table of contents and headings in this Deed do not affect its interpretation;

1 .2.6 writing or written does not include e-mail or any other form of electronic communication, other than fax where explicitly stated;

1 .2.7 the terms including, include, in particular or any similar expression shall be construed as illustrative and shall not limit the sense of the words preceding those terms,

12.8 references to the parties include their respective successors in title, permitted assignees, estates and legal personal representatives;

1 .2.9 unless otherwise specified, a reference to legislation or a legislative provision is a reference to it as amended, consolidated, extended or re-enacted from time to time (whether before or after the date of this Deed) and to any subordinate legislation made under it from time to time; and

1.2.10 if the Sub-Consultant is a partnership each partner shall be jointly and severally liable under this Deed. Where the context so requires and where the Sub-Consultant is a partnership, the term Sub-Consultant shall be deemed to include any additional partner(s) who may be admitted into the partnership of the Sub-Consultant during the currency of this Deed. This Deed shall not automatically terminate upon the death, retirement or resignation of one or more members of such partnership.

2. EXERCISE OF SKILL AND CARE

2.1 The Sub-Consultant warrants and undertakes to the Beneficiary that it has observed and performed and shall continue to observe and perform each and all of its services, duties and obligations contained in or implied by the Contract- Save as expressly provided for in this Deed the duty of the Sub-Consultant is to be treated as being no greater than it would have been if the Beneficiary had been a party to the Contract instead of this Deed but neither this provision nor any other provision in this Deed shall entitle the Sub-Consultant to raise any defence based on set-off or counterclaim and/or prevent the Beneficiary from recovering loss and/or damage from the Sub-Consultant as a result of the Sub-Consultant's breach of any provisions of this Deed on the basis that the Consultant and/or the Employer have not suffered any loss and/or damage and/or the same loss and/or damage and the Sub-Consultant hereby irrevocably agrees and undertakes not to raise any such arguments by way of defence and/or set-off and/or counterclaim to any claim made by the Beneficiary.

2.2 Without prejudice to the generality of Clause 2.1 the Sub-Consultant warrants and undertakes to the Beneficiary that it has exercised and shall continue to exercise in the performance of the services duties and obligations contained in or implied by the Contract all reasonable skill, care and diligence to be expected of a properly qualified and competent consultant experienced in perfornmng similar services, duties and obligations in relation to developments of a similar nature, value, scope, character, complexity and timescale to the Development.

2.3 The Sub-Consultant further warrants and undertakes to the Beneficiary that, in observing and performing each and all of its services, duties and obligations contained in or implied by the Contract, the Sub-Consultant shall comply with all applicable statutory and regulatory

requirements.

2.4 The Sub-Consultant acknowledges that has relied and shall rely on the warranties under this Clause 2 and the other terms of this Deed and may and/or shall suffer loss and/or damage in the event of a breach of these warranties and/or the other terms of this Deed,

2.5 The obligations of the Sub-Consultant under this Deed shall not be released or diminished by the appointment of any person by the Beneficiary to carry out any independent enquiry into any matter.

3. OBLIGATIONS PRIOR TO TERMINATION OF THE CONTRACT

[NOTE - Clauses 3 and 4 (step in rights) are usually only used where the Beneficiary is a purchaser or funder, or to the Employer. If the Beneficiary is not a purchaser or funder, or if they are not to be given step in rights, delete Clause 3, 4 and 13; delete the Consultant details in Clause 9; and delete the Consultant from being a signatory to this collateral warranty on the coversheet, parties and execution clauses, and instead insert a new definition of Consultant with their details in Background A or the table at Clause 1.1]

3.1 The Sub-Consultant warrants and undertakes to the Beneficiary that it shall not exercise or seek to exercise any right of termination of the Contract and/or to discontinue the performance of any of its services, duties and/or obligations thereunder for any reason whatsoever (including any services duties and/or obligations in relation to the Development by reason of breach on the part of the Consultant) without giving to the Beneficiary not less than 28 days' notice of its intention to do so and specifying the grounds for the proposed termination and/or discontinuance.

32 Any period stipulated in the Contract for the exercise by the Sub-Consultant of a right of termination of the Contract and/or to discontinue the performance of any of its services, duties and/or obligations in relation to the Development shall be extended as may be necessary to take account of the period of notice required under Clause 0.

3.3 Compliance by the Sub-Consultant with the provisions of Clause O shall not be treated as a waiver of any breach on the part of the Consultant giving rise to the right of termination of the Contract and/or to discontinue the performance of any of the Sub-Consultant's services, duties and/or obligations in relation to the Development, nor otherwise prevent the Sub-Consultant from exercising its rights after the expiration of the notice unless the right of termination and/or right to discontinue shall have ceased under the provisions of Clause 4.

4, OBLIGATIONS OF THE SUB-CONSULTANT TO THE BENEFICIARY

[NOTE - Clauses 3 and 4 are usually only used where the Beneficiary is a purchaser or funder 1 or to the Employer — see note under Clause 3 above.]

4. 1 The right of the Sub-Consultant to terminate the Contract and/or to discontinue the performance of any of its services, duties and/or obligations shall cease within the period of 28 days referred to in Clause 0 if the Beneficiary shall give written notice to the Sub-Consultant:

4. 1 .1 requiring the Sub-Consultant to continue performing its services, duties and obligations under the Contract in relation to the Development,

4. 1 .2 acknowledging that the Beneficiary is assuming all the services, duties and obligations of the Consultant under the Contract;

4.1 .3 undertaking unconditionally to the Sub-Consultant to discharge all payments which may subsequently become due to the Sub-Consultant under the terms of the Contract;

and shall pay to the Sub-Consultant any sums which have become due and payable to it under the Contract but which were then unpaid*

4.2 Upon compliance by the Beneficiary with the requirements Of Clause O the Contract shall continue in full force and effect as if the right of termination and/or discontinuance on the part of

the Sub-Consultant had not arisen and in all respects as if the Contract had been made between the Sub-Consultant and the Beneficiary to the exclusion of the Consultant.

4.3 Notwithstanding that as between the Consultant and the Sub-Consultant the Sub-Consultant's rights of termination of the Contract and/or discontinuance may not have arisen, the provisions of Clause 4.2 shall nevertheless apply if the Beneficiary gives notice to the Sub-Consultant and the Consultant to that effect and the Beneficiary complies with the requirements on its part under Clause 0.

44 The Sub-Consultant shall not be concerned or required to enquire whether, and shall be bound to assume that, as between the Consultant and the Beneficiary the circumstances have occurred permitting the Beneficiary to give notice under Clause 0.

4.5 The Sub-Consultant acting in accordance with the provisions of this Clause 4 shall not by so doing incur any liability to the Consultant,

4.6 Where the Sub-Consultant has given rights similar to those contained in Clauses 3 and 4 of this Deed to any other person or persons, then if both the Beneficiary and such other person or persons shall serve notice under Clause 0 or its equivalent, the notice served by the Beneficiary [shall prevail over any notice served by any other person or persons / shall not prevail over any notice served by any other person or persons / shall not prevail over any notice served by [o] but shall prevail over any notice served by any other person or persons]. The Sub-Consultant acting in accordance with the provisions of this Clause 4.6 shall not be and shall not be deemed to be in breach of the provisions of this Deed by doing sot nor shall the Sub-Consultant in doing so incur any liability to the Beneficiary,

5. INTELLECTUAL PROPERTY RIGHTS

5.1 The Sub-Consultant with full title guarantee grants to the Beneficiary, with immediate effect, an irrevocable, perpetual, non-exclusive, non-terminable, royalty-free licence to use, reproduce and transmit any or all of the Materials produced or prepared by the Sub-Consultant or on the SubConsultant's behalf for any purpose whatsoever relating to the Development and/or the Site including (without limitation) the design, construction, completion, promotion, advertisement, funding, sale, letting, disposal, fitting out, maintenance, use, occupation, management, repair, reinstatement re-construction, modification, alteration, refurbishment, re-development, decommissioning, demolition and/or extension of the Development and/or the Site. Such licence shall carry the right to grant sub-licences and shall be transferable to third parties without the Sub-Consultant's prior consent and shall subsist notwithstanding the termination (for any reason) of the Contract.

5.2 The Sub-Consultant shall not be liable for the consequences of any use by the Beneficiary of the Materials for any purposes other than those for which the same are or were prepared.

5.3 The Sub-Consultant warrants to the Beneficiary that it is authorised to grant the licence set out in Clause 5.1 in respect of any Materials whose intellectual property rights are vested in any third person and that the use of the Materials for any purpose relating to the Development and/or Site shall not infringe the rights of any third person. If the use of the Materials is found to infringe the rights of any third person, the Consultant shall indemnify the Beneficiary against all resulting claims, proceedings, damages, costs and expenses,

5.4 To the extent that the Sub-Consultant is (or at the time of their creation may be) the author of the Materials, the Sub-Consultant hereby absolutely waives and agrees not to assert any moral rights which it might otherwise be deemed to possess pursuant to the Copyright, Designs and Patents Act 1988 or any equivalent legislation in respect Of the Materials; and to the extent that the SubConsultant is not the author, the Sub-Consultant warrants that the author has not asserted and has waived and agreed to waive any such moral rights which the author might otherwise be deemed to possess.

5.5 The Sub-Consultant agrees:

545. 1 on request at any time to give or any persons authorised by the Beneficiary full and sufficient access to the Materials and, at the Beneficiary's expense, to provide full and proper copies of the Materials (including copy negatives and electronic copies); and

55.2 at the Sub-Consultant's expense, to provide the Beneficiary with a set of all Materials on Practical Completion.

5.6 All royalties or other sums payable in respect of the supply and use of any patented articles, processes or inventions required in connection with the Contract shall be paid by the SubConsultant and the Sub-Consultant shall indemnify the Beneficiary from and against all claims, proceedings, damages, costs and expenses suffered or incurred by the Beneficiary by reason of the Sub-Consultant infringing or being held to infringe any intellectual property rights in the course of or in connection with the Contract.

5.7 The Sub-Consultant shall (subject to the Beneficiary paying the Sub-Consultant's reasonable costs so to do) if reasonably requested by the Beneficiary at any time execute such documents and perform such acts as may be required fully and effectively to assure to the Beneficiary the rights referred to in this Clause 5.

6. INSURANCE

6.1 The Sub-Consultant warrants to the Beneficiary that it maintains, has at all relevant times maintained, and shall continue to maintain throughout the duration of the Development and for a period of 12 years following Practical Completion (irrespective of any termination of the Contract or the Sub-Consultant's employment under the Contract for any reason) professional indemnity insurance with reputable insurers lawfully carrying on such insurance business in the United Kingdom with a limit of indemnity of not less than ECO] pounds) for any one occurrence or series of occurrences arising out of any one event to cover any claims made under this Deed against the Sub-Consultant in relation to the Development.

6.2 The Sub-Consultant shall maintain the professional indemnity insurance on terms and conditions that do not require the Sub-Consultant to discharge any liability before being entitled to recover from the insurers and would not adversely affect the rights of any person to recover from the insurers pursuant to the Third Parties (Rights Against Insurers) Act 2010.

6.3 As and when reasonably required by the Beneficiary the Sub-Consultant shall provide satisfactory documentary evidence of the terms of insurance referred to in Clause 6.1 and that the insurance referred to in Clause 6.1 is being properly maintained, and shall confirm that payment has been made in respect of the last preceding premium due under such insurance.

6.4 The Sub-Consultant warrants that it has at all relevant times observed and shall continue to observe all of the conditions of the insurance policy referred to in Clause I and all of the insurance provisions contained or referred to in the Contract.

6.5 The preceding parts of this Clause 6 shall not apply at times when and to the extent that the insurance referred to in Clause 6.1 is not available in the United Kingdom insurance market at commercially reasonable rates, and the Sub-Consultant has notified the Beneficiary accordingly. upon such notification the Sub-Consultant shall make itself available to the Beneficiary to discuss reasonable means of protecting the Beneficiary and the Sub-Consultant shall take any reasonable steps requested by the Beneficiary. For the purposes of this Clause 6.5, commercially reasonable rates shall mean such level of premium rates at which other consultants and/or sub-consultants of a similar size and financial standing as the Sub-Consultant at each renewal date generally continue to take

out such insurance. For the avoidance of doubti any increased or additional premium required by insurers by reason of the Sub-Consultant's own claims record or other acts, errors, omissions, negligence, breaches, defaults, matters or things particular to the Sub-Consultant shall be deemed to be within commercially reasonable rates.

7.HEALTH AND SAFETY

The Sub-Consultant warrants that it has complied and shall comply with all of its obligations in relation to the Development as set out in the Construction (Design and Management) Regulations 2015.

8. EXCLUDED MATERIALS

8.1 The Sub-Consultant warrants that it has not and shall not use and/or permit the use of and/or specify for use in or in connection with the Development any substances materials equipment products kit practices or techniques which by their nature or application do not conform with relevant British Standards or Codes of Practice or regulations or good building practice or any European Union equivalent current at the time of use or permission or specification, nor any substances materials equipment products kit practices or techniques which are generally known or generally suspected within the Sub-Consultant's trade and/or the construction industry:

8. 1 .1 to be deleterious in the particular circumstances in which they are used or specified for use to the health or safety of any person;

8.1 .2 to be deleterious in the particular circumstances in which they are used or specified for use to the health, safety, stability, performance, physical integrity and/or durability of the Development or any part thereof and/or to other structures, finishes, plant and/or machinery;

8.1 .3 to reduce or possibly reduce the normal life expectancy of developments of a type comparable to the Development;

8.1.4 to become deleterious without a level or cost of maintenance which is higher than that which would normally be expected in a development of a type comparable to the

Development,

8.1 .5 not to comply with or have due regard to the report entitled "Good Practice in the Selection of Construction Materials" (current edition) published by the British Council for Offices; and/or

8, 1 .6 [o be supplied or placed on the market in breach of the Construction Products Regulations.

9. COMMUNICATIONS

9.1 Except as otherwise provided for in this Deed, all notices or other communications under or in respect of this Deed to either party shall be deemed to be duly given or made when:

91.1 delivered (in the case of personal delivery or letter); or

9.1 .2 despatched (in the case of facsimile)

to that party at the address or facsimile number appearing below (or at such other address or facsimile number as that party may hereafter specify for this purpose to the other):

in the case of the Sub-Consultant: [0] [NOTE - name / address / facsimile to be inserted]

in the case of the Beneficiary: (NOTE - name / address / facsimile to be inserted] in the

case of the Consultant: [0] [NOTE - name / address / facsimile to be inserted]

9.2 A written notice includes a notice by facsimile. A notice or other communication which is not received on a Business Day or which is received after business hours in the place of receipt shall be deemed to be given or made on the next following Business Day in that place.

1 0. CONCURRENT LIABILITIES

The rights and benefits conferred upon by this Deed are in addition to any other rights and remedies it may have against the Sub-Consultant including, without prejudice to the generality of the foregoing, any remedies in negligence.

1 1 . ASSIGNMENT

1 1 .1 The Beneficiary may without the consent of the Sub-Consultant assign transfer and/or charge the benefit of all or any of the Sub-Consultants obligations under this Deed and/or any benefit arising under or out of this Deed.

1 1 .1 M by way of security or by way of re-assignment on redemption; and

1 1 .1 2 by absolute assignment to any Group Company of the Beneficiary; and

1 1 .1 .3 by absolute assignment on two other occasions only,

1 1 .2 In this Deed references to the Beneficiary include where the context admits its permitted assignees.

1 1 .3 The Sub-Consultant shall not be entitled to contend that any person to whom this Deed is assigned in accordance with Clause llwl is precluded from recovering under this Deed any loss incurred by such assignee resulting from any breach of this Deed (whenever happening), by reason that such person is an assignee and not a named party under this Deed.

1 1 .4 The Sub-Consultant shall not be entitled to assign, transfer and/or charge the benefit of any (if any) of the Beneficiary's obligations under this Deed and/or any benefit (if any) arising to the SubConsultant out of this Deed.

12. LIMITATION PERIOD

The liability of the Sub-Consultant under this Deed shall cease 12 years following Practical Completion save in relation to any claims made by the Beneficiary against the Sub-Consultant and/or notified by the Beneficiary to the Sub-Consultant in writing prior thereto. For the avoidance of doubt, the parties agree that any provisions of the Limitation Act 1980 to the contrary will not apply to this Deed.

13. CONSULTANT

[NOTE - delete if Clauses 3 and 4 are deleted]

The Consultant agrees that it shall not take any steps which would prevent or hinder the Beneficiary from exercising its rights under this Deed and confirms that the rights of the Beneficiary in Clauses 3 and 4 override any obligations of the Sub-Consultant to the Consultant under the Contract

14. GOVERNING LAW AND JURISDICTION

1 4.1 This Deed and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) is governed by and construed in accordance With the law of England and Wales.

1 4.2 The parties irrevocably agree that the courts of England and Wales shall have exclusive jurisdiction to hear and decide any suit, action or proceedings and/or settle any dispute or claim arising out of or in connection with this Deed or its subject matter or formation (including noncontractual disputes or claims).

15. RIGHTS OF THIRD PARTIES

Unless the right of enforcement is expressly provided for, no third party (as defined in the Contracts (Rights of Third Parties) Act 1999) except for any permitted successor or assignee of any party to this Deed has any rights under that Act to enforce any term of this Deed.

This document has been executed as a deed and is delivered and takes effect on the date stated at the beginning of it.

acting by [insert name of first director], a director

and [insert name of second director or secretary] [a director/its secretary]

.....

Director

[Director/Secretary]

OR

Executed as a deed by [insert name of company] acting by [insert name of director], a director, in the presence of [insert name of witness]:

.....

Director

Executed as a deed by [insert name of company]

Signature (Witness).....

Print Name.....

Address.....

Occupation .....

Annex E

Prglegt Team Members

[redacted] [redacted] — [redacted]

Survey Team

[redacted] — [redacted]

[redacted] — [redacted]

[redacted] — [redacted]

[redacted] — [redacted]

Annex F

Financial Distress

I, Definitions

I In this Schedule [I the following definitions apply:

"Credit Rating Threshold" means the minimum credit rating level for the Consultant as set out in Annex 1

"Financial Distress Event" means the occurrence or one or more of the events listed in this Schedule [ ]

"Financial Distress Service Continuity Plan" means a plan setting out how the Consultant will ensure the continued performance in accordance with this contract in the event that a Financial Distress Event occurs;

"Rating Agency" means the rating agency means Dun & Bradstreet.

2. Credit rating and duty to notify

2.1. The Consultant warrants and represents to the Client for the benefit of the Client that as at the Contract Date the long-term credit ratings issued for the Consultant by the Rating Agency.

2.2. The Consultant promptly notifies (or procures that its auditors promptly notify) the Client if there is any significant downgrade in the credit rating issued by any Rating Agency for the Consultant (and in any event within seven days from the occurrence of the downgrade).

2.3, If there is any downgrade credit rating issued by any Rating Agency for the Consultant, the Consultant ensures that the Consultant's auditors thereafter provide the Client within 14 days of a written request by the Client with written calculations of the quick ratio for the Consultant at such date as may be requested by the Client For these purposes the "quick ratio" on any date means: Where

A. is the value at the relevant date of all cash in hand and at the bank of the Consultant

B. is the value of all marketable securities held by the Consultant determined using closing prices on the working day preceding the relevant date

C. is the value at the relevant date of all account receivables of the Consultant and

D. is the value at the relevant date of the current liabilities of the Consultant

2.4. The Consultant.

- regularly monitors the credit ratings of the Consultant with the Rating Agencies and
- promptly notifies (or shall procure that its auditors promptly notify) the Client following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event and in any event, shall ensure that such notification is made within 14 days of the date on which the Consultant first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event.

2.5. For the purposes of determining whether a Financial Distress Event has occurred pursuant to the provisions of paragraph, the credit rating of the Consultant shall be deemed to have dropped below the applicable Credit Rating Threshold if any of the Rating Agencies have rated the Consultant at or below the applicable Credit Rating Threshold.

3. Consequences of a financial distress event

3.1. In the event of.

3.1 41 . the credit rating of the Consultant dropping below the applicable Credit Rating Threshold;

3.1 . 2. the Consultant issuing a profits warning to a stock exchange or making any other public announcement about a material deterioration in its financial position or prospects;

3.1 *3. there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Consultant;

3m 1.4. the Consultant committing a material breach of covenant to its lenders,

3.1.5. a Sub-contractor notifying the Client that the Consultant has not satisfied any sums properly due for a material specified invoice or sequences of invoices that are not subject to a genuine dispute;

3.1.6. any of the following:

commencement of any litigation against the Consultant with respect to financial indebtedness or obligations under this contract; non-payment by the Consultant of any financial indebtedness; any financial indebtedness of the Consultant becoming due as a result of an event of default the cancellation or suspension of any financial indebtedness in respect of the Consultant in each case which the Client reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance of the Consultant in accordance with this contract

then, immediately upon notification of the Financial Distress Event (or if the Client becomes aware of the Financial Distress Event without notification and brings the event

to the attention of the Consultant), the Consultant shall have the obligations and the Client shall have the rights and remedies as set out in paragraphs 3.2 — 3.6

3.2. The Consultant:

3.2M at the request of the Client meets the Client as soon as reasonably practicable (and in any event within three working days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Client may permit and notify to the Consultant in writing) to review the effect of the Financial Distress Event on its continued performance in accordance with this contract and

3.22. where the Client reasonably believes (taking into account any discussions and representations under paragraph 32.1) that the Financial Distress Event could impact on the Consultant's continued performance in accordance with this Contract:

submits to the Client for approval, a draft Financial Distress Service Continuity Plan as soon as reasonably practicable (and in any event, within 14 days from the initial notification (or awareness) of the Financial Distress Event or such other period as the Client may permit and notify to the Consultant in writing) provides such financial information relating to the Consultant as the Client may reasonably requires.

3.3. The Client does not withhold approval of a draft Financial Distress Service Continuity Plan unreasonably. If the Client does not approve the draft Financial Distress Service Continuity Plan, the Client informs the Consultant of the reasons and the Consultant takes those reasons into account in the preparation of a further draft Financial Distress Service Continuity Plan, which the Consultant resubmits to the Client within seven days of the rejection of the first or subsequent (as the case may be) drafts. This

process is repeated until the Financial Distress Service Continuity Plan is approved by the Client or referred to the dispute resolution procedure.

3.4. If the Client considers that the draft Financial Distress Service Continuity Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not remedy the relevant Financial Distress Event, the Client may either agree a further time period for the development and agreement of the Financial Distress Service Continuity Plan or escalate any issues with the draft Financial Distress Service Continuity Plan using the dispute resolution procedure.

3.5. Following approval of the Financial Distress Service Continuity Plan by the Client, the Consultant reviews on a regular basis (which shall not be less than monthly) the Financial Distress Service Continuity Plan and assesses whether it remains adequate and up to date to ensure the continued performance in accordance with this Contract

where the Financial Distress Service Continuity Plan is not adequate or up to date in, submits an updated Financial Distress Service Continuity Plan to the Client for approval, and the provisions of shall apply to the review and approval process for the updated Financial Distress Service Continuity Plan and

complies with the Financial Distress Service Continuity Plan (including any updated Financial Distress Service Continuity Plan).

3.6. Where the Consultant reasonably believes that the relevant Financial Distress Event (or the circumstance or matter which has caused or otherwise led to it) no longer exists, the Consultant notifies the Client and subject to the agreement of the Client, the Consultant is relieved of its obligations under paragraph 3.

4. Termination rights

4.1 . The Client may terminate the Consultant's obligation to perform the Services if

the Consultant fails to notify the Client of a Financial Distress Event in accordance with paragraph 2.2;

the Client fails to agree a Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with paragraph 3 and/or

the Consultant fails to comply with the terms of the Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with paragraph 3.

5. Primacy of credit ratings

5.1 Without prejudice to the Consultant's obligations and the Client's rights and remedies under paragraph 3, if, following the occurrence of a Financial Distress Event pursuant to paragraph 2 to the Rating Agencies review and report subsequently that the credit ratings do not drop below the relevant Credit Rating Threshold, then:

the Consultant is relieved automatically of its obligations under paragraph 3 and the Client is not entitled to require the Consultant to provide financial information in accordance with paragraph 23,

ANNEX 1: CREDIT RATINGS & CREDIT RATING THRESHOLDS

Consultant Credit current rating (long term) [ ]

AC 172319460

Credit Rating Threshold [ ]

Annex G

Security Provisions

1 . Definitions

1.1 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/governmentbaseline-personnel-securitv-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: htt s//www.ncsc. ov.uk/scheme/certified-c berconsultancy
"Buyer"	the Client
"CCFN' "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/abaut-certifiedprofessional-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.cvberessentials.ncsc.gov.uk/gettingcertified/#what-is-an-accreditation-bady

'Data Controller" 'Data Protection Officer' "Data Processor" "Personal Data" "Personal Data requiring Sensitive Processing" "Data Subject", ß 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://wwwgov.uk/government/publications/governmentsecuritv-classificatians

	Her Majesty ᵛs 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 Infdrmation Assurance. The NCSC website is htt s ᵣ.//www.ncsc. ov.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'V "Role Based Access Control"	Role Based Access Control, a method of restricting a person's or process ⁱ access to information depending on the role or functions assigned to them.
"Storage Area Network" "SAN"	an information storage system typically presenting blockbased 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.

AC_17231946ÖO

	NCSC Guidance can be found at: https://wwwrncsc.qcv.uk/quidance/secure-sanitisationstorage-media The disposal of physical documents and hardcopy materials advice can be found at: htt s- //www c nil ov.uk/secure-destruction-0
"Security and Information Risk Advisor" "CCP SIRR "SRA"	the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also: https//www.ncscrqovuk/articles/about-certifiedprofessional-scheme
"Senior Information Risk Owner" "SRO"	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)i 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 assets will apply protective security to ensure HMG can function effectively, efficiently, and securely https://www.qov.uklqavernment/publications/securitvpolicv-framework
"Supplier"	the Consultant
"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.

Operative Provisions

1 . 1 . The Supplier shall be aware of and comply with the relevant HMG securitv policv framework, NCSC quidelines and where applicable these Departmental Security Requirements which include but are not constrained to the following paragraphs.

19. 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 Cvber Essentials Scheme (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.

1 .3. Where paragraph 1.2 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).

1.4. The Supplier shall follow the UK Government Security Classification Policy (GSC?) 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).

1.5. 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 1.14. For information stored digitally, this must be at a minimum logically separated. Physical information (e.g., paper) must be physically separated.

1.6. 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.

1.6.1. 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.

1 .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.

1 .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 .8. 1 . physical security controls;

1 .82. good industry standard policies and processes;

1 .8.3. malware protection;

1.84. boundary access controls including firewalls, application gateways, etc;

1 .8.5. maintenance and use of fully supported software packages in accordance with vendor recommendations;

1 .8.6. use of secure device configuration and builds;

1 .8.7. software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;

1 .8.8. user identity and access controls, including the use of multi-factor authentication for sensitive data and privileged account accesses;

1 .8.9. 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 .8.9. 1 . retained and protected from tampering for a minimum period of six months;

1 .8.9.2. made available to the Buyer on request.

1 .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.

1 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.

1 . 1 1 . 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://wwvvrncsc.gov.uk/guidance/end-userdevice-securitv and https://www.ncsc.gov.uk/callection/end-user-device-securitv/eudoverview/eud-securitv-principles.

1 . 1 2. 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 crosscut 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 , 1 3- 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 . 14. 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 1.15.

1 . 1 5. 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 legali 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 . 1 6. 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.

I T1 7, All Supplier Staff who handle Buyer's Data shall have annual awareness training in protecting informatiom

1418. 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 mightl 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.

1 .1 9. 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 and followed up in writing. If Security Incident reporting has been delayed by more than 24 hours

the Supplier should provide an explanation about the delay. Regular updates on the Security Incident shall be provided to the Buyer in writing until the incident is resolved.

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 .20. 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 (I THC) using an NCSC CHECK Scheme I THC 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 I THC findings.

1 .21. 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.

1 .22, 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 Annen

1 .23. 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. Th is 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.

1 .24. 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 .24, 1 , implementation Of the foundational set Of cyber defence safeguards from the Center for Internet Security Critical Security Controls (CIS CSC v8).

1 24.2. any existing security assurance for the Services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification issued by an organisation accredited by the United Kingdom Accreditation Service.

1 .24.3. 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.

1 .24.4. 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.

1.24.5. compliance with the principles of Secure by Design as described at Secure by Design Principles - UK Government Security.

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.

1.25. 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,

1 .26. The Supplier shall comply with the NCSCs social media guidance: how to use social media 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.

1 .27. 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,

1.28. Where the Supplier is using Artificial Intelligence (Al) 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.

Annex H

GDPR

The following definitions shall apply to this Annex H

Agreement this contract;

Processor Personnel : means all directorst officers, employees, agents, consultants and Consultants of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Agreement.

GDPR CLAUSE DEFINITIONS:

Data Protection Legislation (i) the GDPR, (ii) the DPA 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 which, pending a decision from the competent authorities of the ELI on the adequacy of the UK data protection regime will include the requirements set out or referenced in Part Three, Title Vll, Article 71 (1) of the Withdrawal Agreement signed by the UK and the EU in December 2019 ;

Data Protection Impact Assessment : an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

Controller , Processor , Data Subject Personal Data , Personal Data Breach Data Protection Officer take the meaning given in the GDPR

Data Loss Event : any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

Data Subject 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.

DPA 2018 : Data Protection Act 2018

GDPR : the General Data Protection Regulation (Regulation (ELI) 2016/679) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019

Joint Controllers: where two or more Controllers jointly determine the purposes and means of processing

Protective Measures : appropriate technical and organisatlonal 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 including those outlined in Schedule 1 to this Annex (Security).

Sub-processor : any third party appointed to process Personal Data on behalf of that Processor related to this Agreement

1. DATA PROTECTION

I . I The Parties acknowledge that for the purposes of the Data Protection Legislation, the Client is the Controller and the Consultant is the Processor unless otherwise specified in Schedule 1 to this Annex. The only processing that the Processor is authorised to do is listed in Schedule 1 to this Annex by the Controller and may not be determined by the Processor.

1.2The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

1.3The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

(a) process that Personal Data only in accordance with Schedule 1 to this Annex , unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, are appropriate to protect against a Data Loss Event, 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:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and (iv)cost of implementing any measures;

(c) ensure that :

(i) the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule 1 to this Annex);

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Processor's duties under this clause;

(B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

(C)are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data; and

(d) not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer
(in accordance with the Data Protection Legislation) as determined by the Controller;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) 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

(iv)the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

(e) at the written direction Of the Controller1 delete or return Personal Data (and any copies Of it) to the Controller on termination of the Agreement unless the Processor is required by Law to retain the Personal Data.

1 .5 Subject to clause 1.6, the Processor shall notify the Controller immediately if it:

(a) receives a Data Subject Request (or purported Data Subject Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

(f) becomes aware of a Data Loss Event.

1 .6 The Processor's obligation to notify under clause 1.5 shall include the provision of further information to the Controller in phases, as details become available.

1 7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1 .5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

(a) the Controller with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Controller following any Data Loss Event,

(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

1.8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

(a) the Controller determines that the processing is not occasional;

(b) the Controller determines the processing includes special categories of data as referred to in Article) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or

(c) the Controller determines that the processing is likely to result in a risk to the rights and freedoms Of Data Subjects.

1.9The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

1 .1 0 Each Party shall designate its own data protection officer if required by the Data Protection Legislation .

1 .1 1 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:

(a) notify the Controller in writing of the intended Sub-processor and processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause such that they apply to the Sub-processor; and

(d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

1 .12 The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

1 .1 3 The Controller may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

1 .14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

1 &1 5 Where the Parties include two or more Joint Controllers as identified in Schedule [Xl in accordance with GDPR Article 26, those Parties shall enter into a Joint Controller Agreement based on the terms outlined in Schedule [Y] in replacement of Clauses 1.1-1.14 for the Personal Data under Joint Control.

Annex H - Part 2: Schedule of Processing, Personal Data and Data Subjects

Schedule 1 Processing, Personal Data and Data Subjects

The Parties do not anticipate that this Contract will involve any processing of Personal Data by the Contractor on behalf of the Employer, and the Contractor is not authorised by the Employer to process Personal Data under the terms of this Contract. The remainder of this Schedule will only be completed and have effect if the Employer instructs the Contractor to process Personal Data under the terms of this Contract.

This Schedule 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 Schedule shall be with the Controller at its absolute discretion.

1 . The contact details of the Controller's Data Protection Officer are: [Insert Contact details]

2. The contact details of the Processor's Data Protection Officer are: [Insert Contact details]

3. The Processor shall comply with any further written instructions with respect to processing by the Controller.

4 Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Consultant is the Processor in accordance with Clause 1 . 1 . [Guidance: You may need to vary this section where (in the rare case) the Customer and Consultant have a different relationship. For example where the Parties are Joint Controller of some Personal Data, "Notwithstanding Clause 1 .1 the Parties acknowledge that they are also Joint Controllers for the purposes of the Data Protection Legislation in respect of: [Insert the scope of Personal Data which the purposes and means of the processing is determined by the both Parties] In respect of Personal Data under Joint Control, Clause 1.115 will not apply and the Parties agree to put in place a Joint Controller Agreement as outlined in Schedule Y instead."
Subject matter of the processing	[This should be a high level, short description of what the processing is about i.e. its subject matter of the contract. Example: The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide a service to members of the public.]
Duration of the processing	[Clearly set out the duration of the processing including dates]
Nature and purposes of the processing	[Please be as specific as possible, but make sure that you cover all intended purposes. The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc. The purpose might include: employment processing, statutory obligation, recruitment assessment etc]
Type of Personal Data being Processed	[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]

Categories of Data Subject	(Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / u ils, members of the ublic, users of a

1/2319460

	particular website etc]
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	[Describe how long the data will be retained for, how it be returned or destroyed]

AC 1 72319460 2