# DPS Schedule 6 (Order Form Template and Order Schedules)

## Order Form

**ORDER REFERENCE:** CCSO20A47

**THE BUYER:** Crown Commercial Service

**BUYER ADDRESS**:
REDACTED

**THE SUPPLIER**: Cognizant Worldwide Limited

**SUPPLIER ADDRESS:**
REDACTED

**REGISTRATION NUMBER: REDACTED**

**DUNS NUMBER: REDACTED**

**DPS SUPPLIER REGISTRATION SERVICE ID: REDACTED**

**APPLICABLE DPS CONTRACT**

This Order Form is for the provision of the Deliverables and dated 1st July 2020. It's issued under the DPS Contract with the reference number RM6148 for the provision of Quality Assurance & Testing for IT Systems 2.

**DPS FILTER CATEGORY (IES):**

Not Applicable

**ORDER INCORPORATED TERMS**
The following documents are incorporated into this Order Contract. Where numbers are missing we are not using those Schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Order Special Terms and Order Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM6148
3. The following Schedules in equal order of precedence:

Joint Schedules for RM6148
- Joint Schedule 2 (Variation Form)

Order Schedules for RM6148
- Order Schedule 5 (Pricing Details)
- Order Schedule 7 (Key Supplier Staff)
- Order Schedule 14 (Service Levels)
- CCS Core Terms (DPS version)

DPS Schedules RM6148
- DPS Schedule 1 (Specification)
- DPS Schedule 3 (DPS Pricing)

No other Supplier terms are part of the Order Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

**ORDER SPECIAL TERMS**
None

ORDER START DATE: 2nd July 2020

ORDER EXPIRY DATE: 28th November 2020

ORDER INITIAL PERIOD: 6 month period.

ORDER OPTIONAL EXTENSION: Not Applicable

**DELIVERABLES**
Please see DPS Schedule 1 (Specification) for deliverables.

**MAXIMUM LIABILITY**

.

Clause 11.2 of the Core Terms shall be amended as follows:

"Each Party's total aggregate liability under each Contract Order (whether is contract, tort or otherwise) is no more than 100% of the Charges paid under the Contract Order".

Clause 11.5 of the Core Terms shall be amended as follows:

"In spite of Clauses 11.1 and 11.2, the Supplier does not limit or exclude it's liability for the indemnities in 7.5 and 9.5"

**ORDER CHARGES**

Please see Order Schedule 5 for pricing.

**REIMBURSABLE EXPENSES**

None

**PAYMENT TERMS**

Payment will be made on a Fixed Price basis on the satisfactory delivery of pre-agreed certified products and deliverables.

Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed.

Invoices can be submitted monthly in arrears and payments will be made monthly in arrears on the basis of the following:

65% of fee after report of the full initial audit review has been completed and the reports have been provided to the Authority;

25% of fee per completed audit after re-test and report as been provided to the Authority; and If there is no need for retesting of any systems, then the Authority will agree a payment date with the supplier.

10% of all remaining fees on the delivery of the final report and handover.

**PAYMENT METHOD**

Payment via BACS

**BUYER'S INVOICE ADDRESS:** send through email to

**REDACTED**

**BUYER'S AUTHORISED REPRESENTATIVE:**

REDACTED

**BUYER'S ENVIRONMENTAL POLICY**

Not Applicable

**BUYER'S SECURITY POLICY**

CCS Cloud Security Policy –

CCS Information Security Policy -

**BESPOKE ISMS REQUIRED**

No

**SUPPLIER'S AUTHORISED REPRESENTATIVE**

**SUPPLIER'S CONTRACT MANAGER**

REDACTED

**PROGRESS REPORT FREQUENCY**

REDACTED

Not Applicable

**PROGRESS MEETING FREQUENCY**

The supplier will liaise with the Authority's project manager to report progress in a weekly telephone conference review meeting on the delivery of the work and the requirement. The supplier may also be asked to dial into monthly Steering Group calls. The Supplier will be given sufficient notice before each call

**KEY STAFF**

Not Applicable

**KEY SUBCONTRACTOR(S)**

Not Applicable

**COMMERCIALLY SENSITIVE INFORMATION**

Please see Order Schedule 5 (Pricing Details) and Annex 1 Quality Response

**SERVICE CREDITS**

Please see Order Schedule 14

**ADDITIONAL INSURANCES**
Not Applicable

**GUARANTEE**
Not Applicable

**SOCIAL VALUE COMMITMENT**
Not Applicable

| **For and on behalf of the Supplier:** | | **For and on behalf of the Buyer:** | |
|---|---|---|---|
| Signature: | REDACTED | | REDACTED |
| Name: | REDACTED | Name: | REDACTED |
| Role: | Authorized Person | Role: | Head of Project Accounting |
| Date: | Jul 22, 2020 | Date: | Aug 5, 2020 |

## Joint Schedule 2 (Variation Form)

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the Contract)

### Contract Details

| | |
|---|---|
| This Variation is between: | CCS ("CCS" "the Buyer")<br><br>Cognizant Worldwide Limited ("the Supplier") |
| Contract Name: | Provision of Audit/Testing for Adherence to WCAG 2.1 AA Regulations |
| Contract Reference Number: | CCSO20A47 |

### Details of Proposed Variation

| | |
|---|---|
| Variation initiated by: [delete as applicable: CCS/Buyer/Supplier] | Insert |
| Variation number: [insert variation number] | Insert |
| Date variation is raised: [insert date] | Insert |
| Proposed variation | Insert |
| Reason for the variation: [insert reason] | Insert |
| An Impact Assessment shall be provided within: | Insert |

### Impact of Variation

| | |
|---|---|
| Likely impact of the proposed variation: | [Supplier to insert assessment of impact] |

### Outcome of Variation

| | |
|---|---|
| Contract Variation | This Contract detailed above is varied as follows:<br><br>[CCS/Buyer to insert original Clauses or Paragraphs to be varied and the changed clause] |
| Financial Variation | Original contract value<br>£XXX |
| | Additional cost due to variation |

| | |
|---|---|
| | £XXX |
| | New Contract Value<br>£XXX |

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by Buyer

2. Words and expressions in this Variation shall have the meanings given to them in the Contract.

3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the Buyer
Signature

Date

Name (in Capitals)

Address

Signed by an authorised signatory to sign for and on behalf of the Supplier
Signature

Date

Name (in Capitals)

Address

# Joint Schedule 7 – Financial Difficulties

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

**"Credit Rating Threshold"**

**T**he minimum credit rating level for the Monitored Company as set out in the third Column of the table at Annex 2 and

**"Financial Distress Event"**

The occurrence or one or more of the following events:

a) the credit rating of the Monitored Company dropping below the applicable Credit Rating Threshold;

b) the Monitored Company issuing a profits warning to a stock exchange or making any other public announcement about a material deterioration in its financial position or prospects;

c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Monitored Party;

d) Monitored Company committing a material breach of covenant to its lenders;

e) a Key Subcontractor (where applicable) notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute; or

f) any of the following:

i) commencement of any litigation against the Monitored Company with respect to financial indebtedness or obligations under a contract;

ii) non-payment by the Monitored Company of any financial indebtedness;
iii) any financial indebtedness of the Monitored Company becoming due as a result of an event of default; or
iv) the cancellation or suspension of any financial indebtedness in respect of the Monitored Company
In each case which CCS reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance of any Contract and delivery of the Deliverables in accordance with any Order Contract;

"**Financial Distress Service Continuity Plan"**

A plan setting out how the Supplier will ensure the continued performance and delivery of the Deliverables in accordance with each Order Contract in the event that a Financial Distress Event occurs;

"**Monitored Company**"
Supplier/[the DPS Guarantor/ [and Order Guarantor] or any Key Subcontractor]

**"Rating Agency"** The rating agency stated in Annex 1.

2. When this Schedule applies

2.1 The Parties shall comply with the provisions of this Schedule in relation to the assessment of the financial standing of the Monitored Companies and the consequences of a change to that financial standing.

2.2 The terms of this Schedule shall survive termination or expiry of this Contract.

3. What happens when your credit rating changes

3.1 The Supplier warrants and represents to CCS that as at the Start Date the credit rating issued for the Monitored Companies by the Rating Agency is as set out in Annex 2.

3.2 The Supplier shall promptly (and in any event within ten (10) Working Days) notify CCS in writing if there is any downgrade in the credit rating issued by the Rating Agency for a Monitored Company which means that the credit rating for the Monitored company falls below the Credit Rating Threshold.

3.3 If there is any such downgrade credit rating issued by the Rating Agency for a Monitored Company the Supplier shall at CCS' request ensure that the Monitored Company's auditors thereafter provide CCS within 10 Working Days of the end of each Contract Year and within 10 Working Days of written request by CCS (such requests not to exceed 4 in any Contract Year) with written calculations of the quick ratio for the Monitored Company as at the end of each Contract Year or such other date as may be requested by CCS. For these purposes the "quick ratio" on any date means:

A Is the value at the relevant date of all cash in hand and at the bank of the Monitored Company];

B Is the value of all marketable securities held by the Supplier the Monitored Company 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 Monitored]; and

D Is the value at the relevant date of the current liabilities of the Monitored Company].

3.4 The Supplier shall:

3.4.1 Regularly monitor the credit ratings of each Monitored Company with the Rating Agency; and

3.4.2 Promptly notify (or shall procure that its auditors promptly notify) CCS in writing 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, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event.

3.5 For the purposes of determining whether a Financial Distress Event has occurred the credit rating of the Monitored Company shall be deemed to have dropped below the applicable Credit Rating Threshold if the Rating Agency has rated the Monitored Company at or below the applicable Credit Rating Threshold.

4. What happens if there is a financial distress event

4.1 In the event of a Financial Distress Event then, immediately upon notification of the Financial Distress Event (or if CCS becomes aware of the Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and CCS shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.

4.2 In the event that a Financial Distress Event arises due to a Key Subcontractor notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute then, CCS shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier ten (10) Working Days to:

4.2.1 Rectify such late or non-payment; or

4.2.2 Demonstrate to CCS's reasonable satisfaction that there is a valid reason for late or non-payment.

4.3 The Supplier shall and shall procure that the other Monitored Companies shall:

4.3.1 At the request of CCS meet CCS as soon as reasonably practicable (and in any event within three (3) Working Days of the initial notification (or awareness) of the Financial Distress Event) to review the effect of the Financial Distress Event on the continued performance of each Contract and delivery of the Deliverables in accordance each Call-Off Contract; and

4.3.2 Where CCS reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1) that the Financial Distress Event could impact on the continued performance of each Contract and delivery of the Deliverables in accordance with each Call-Off Contract:

(a) Submit to CCS for its Approval, a draft Financial Distress Service Continuity Plan as soon as reasonably practicable (and in any event, within ten (10) Working Days of the initial notification (or awareness) of the Financial Distress Event); and

(b) Provide such financial information relating to the Monitored Company as CCS may reasonably require.

4.4 If CCS does not (acting reasonably) approve the draft Financial Distress

Service Continuity Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Service Continuity Plan, which shall be resubmitted to CCS within five (5) Working Days of the rejection of the first or subsequent (as the case may be) drafts. This process shall be repeated until the Financial Distress Service Continuity Plan is Approved by CCS or referred to the Dispute Resolution Procedure.

4.5 If CCS 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, then it 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.

4.6 Following Approval of the Financial Distress Service Continuity Plan by CCS, the Supplier shall:

4.6.1 on a regular basis (which shall not be less than Monthly), review the Financial Distress Service Continuity Plan and assess whether it remains adequate and up to date to ensure the continued performance each Contract and delivery of the Deliverables in accordance with each Call-Off Contract;

4.6.2 where the Financial Distress Service Continuity Plan is not adequate or up to date in accordance with Paragraph 4.6.1, submit an updated Financial Distress Service Continuity Plan to CCS for its Approval, and the provisions of Paragraphs 4.5 and 4.6 shall apply to the review and Approval process for the updated Financial Distress Service Continuity Plan; and

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

4.7 Where the Supplier reasonably believes that the relevant Financial Distress Event (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify CCS and subject to the agreement of the Parties, the Supplier may be relieved of its obligations under Paragraph 4.6.

4.8 CCS shall be able to share any information it receives from the Supplier in accordance with this Paragraph with any Buyer who has entered into a CallOff Contract with the Supplier.

5. When CCS or the Buyer can terminate for financial distress

5.1 CCS shall be entitled to terminate this Contract and Buyers shall be entitled to terminate their Call-Off Contracts for material Default if:

5.1.1 the Supplier fails to notify CCS of a Financial Distress Event in accordance with Paragraph 3.4;

5.1.2 CCS and the Supplier fail to agree a Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraphs 4.3 to 4.5; and/or

5.1.3 the Supplier 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 4.6.3.

6. What happens If your credit rating is still good

6.1 Without prejudice to the Supplier's obligations and CCS' and the Buyer's rights and remedies under Paragraph 5, if, following the occurrence of a Financial Distress Event, the Rating Agency reviews and reports subsequently that the credit rating does not drop below the relevant Credit Rating Threshold, then:

6.1.1 the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.6; and

6.1.2 CCS shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3.2(b).

## Annex 1: RATING AGENCY

Dun & Bradstreet

## Annex 2: CREDIT RATINGS & CREDIT RATING THRESHOLDS

Part 1: Current Rating

| Entity | Credit Rating | Credit Rating Threshold |
|---|---|---|
| Supplier | Dun & Bradstreet | 35 |

# Joint Schedule 11 (Processing Data) – Non-Applicable

**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 a Contract dictates the status of each party under the DPA. A Party may act as:

(a) "Controller" in respect of the other Party who is "Processor"; (b) "Processor" in respect of the other Party who is "Controller";
(c) "Joint Controller" with the other Party;
(d) "Independent Controller" of the Personal Data where the other Party is also "Controller",

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

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

2. Where a Party is a Processor, the only processing that it is authorised to do is listed in Annex 1 (Processing Personal Data) by the Controller.

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

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

(a) a systematic description of the envisaged Processing and the purpose of the Processing;
(b) an assessment of the necessity and proportionality of the Processing 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.

5. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

(a) Process that Personal Data only in accordance with Annex 1 (Processing Personal Data), 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, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, 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 the Contract (and in particular Annex 1 (Processing Personal Data));
(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 Joint Schedule 11, Clauses 14 (Data protection), 15 (What you must keep confidential) and 16 (When you can share information);
(B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
(D) have undergone adequate training in the use, care, protection and handling of Personal Data;

(d) 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:

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) 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; and

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

6. Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract 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 the Contract;
(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
(f) becomes aware of a Data Loss Event.

7. The Processor's obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller in phases, as details become available.

8. Taking into account the nature of the Processing, the Processor shall provide the Controller with reasonable assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Joint Schedule 11 (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 it 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; and/or

(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.

9. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

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

(b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the 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.

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

11. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

12. Before allowing any Sub-processor to Process any Personal Data related to the Contract, the Processor must:

(a) notify the Controller in writing of the intended Subprocessor and Processing;

(b) obtain the written consent of the Controller;
(c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and
(d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

13.The Processor shall remain fully liable for all acts or omissions of any of its Sub processors.

14.The Relevant Authority may, at any time on not less than 30 Working Days' notice, revise this Joint Schedule 11 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 Contract).

15.The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than 30 Working Days' notice to the Supplier amend the 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

16.In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11 (Processing Data). Independent Controllers of Personal Data

17.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.

18.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.

19.Where a Party has provided Personal Data to the other Party in accordance with paragraph 7 of this Joint Schedule 11 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.

20. The Parties shall be responsible for their own compliance with Articles 13 and 14 of the GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

21. The Parties shall only provide Personal Data to each other:

(a) to the extent necessary to perform their respective obligations under the Contract;

(b) 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 GDPR); and

(c) where it has recorded it in Annex 1 (Processing Personal Data).

22. 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 GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the GDPR.

23. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 of the GDPR and shall make the record available to the other Party upon reasonable request.

24. 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 Contract ("Request Recipient"):

(a) 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

(b) 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:

(i) 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

(ii) 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.

25. 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 Contract and shall:

(a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

(b) implement any measures necessary to restore the security of any compromised Personal Data;

(c) 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

(d) 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.

26. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 (Processing Personal Data).

27. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 (Processing Personal Data).

28. Notwithstanding the general application of paragraphs 2 to 15 of this Joint Schedule 11 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 paragraphs16 to 27 of this Joint Schedule 11.

**Annex 1 - Processing Personal Data a) Template**

1. The contact details of the Customer's Data Protection Officer is:

   **Jack Foulkes, Crown Commercial Service**

2. The contract details of the Supplier Data Protection Officer is:

   **Simon White, Cognizant (Dataprotectionofficer@cognizant.com)**

   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 Annex.

| **Contract Reference:** | **CCSO20A47** |
|---|---|
| **Date:** | **28/05/2020** |
| **Description Of Authorised Processing** | **Details** |
| Identity of the Controller and Processor | REDACTED, Crown Commercial Service |
| Subject matter of the processing | CCS has a legal requirement to review CCS's digital platform forms (websites and documents which can be accessed by the public and by internal stakeholders) to ensure that they are accessible in line with legal mandate. |
| Duration of the processing | Must be completed by 23 September 2020 |

| | |
|---|---|
| Nature and purposes of the processing | Legal requirement |
| Type of Personal Data | This exercise will not involve personal data. |
| Categories of Data Subject | N/A |
| Plan or return or destruction of the data | N/A |

**Annex 2 - Joint Controller Agreement**

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2-15 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 17-27 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [Supplier/Relevant Authority]:

(a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the GDPR regarding the exercise by Data Subjects of their rights under the GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable

alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR;
(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and
(e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier's/Relevant Authority's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. Undertakings of both Parties

2.1 The Supplier and the Relevant Authority each undertake that they shall:

(a) report to the other Party every [x] months on:

(i) the volume of Data Subject Request (or purported Data Subject Requests) from Data Subjects (or third parties on their behalf);
(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;
(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,that it has received in relation to the subject matter of the Contract during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject before disclosing or transferring the Personal Data to the third party. For the avoidance of doubt to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;
(e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;
(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
(g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

(i) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;

(iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event 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;
(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and
(j) ensure that it notifies the other Party as soon as it becomes aware of Data Loss Event.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

3. Data Protection Breach

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;
(b) all reasonable assistance, including:
(i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
(ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;
(iii) co-ordination with the other Party regarding the management of public

relations and public statements relating to the Personal Data Breach; and/or

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Paragraph 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

4. Audit

4.1 The Supplier shall permit:

(a) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

(b) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under

the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

(a) provide all reasonable assistance to the each other to prepare any data protection impact assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risksand measures); and

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 GDPR.

6. ICO Guidance

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. Liabilities for Data Protection Breach

7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("Financial Penalties") then the following shall occur:

(a) if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at

the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

(b) if in the view of the Information Commissioner, the Supplier is responsible for

the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(c) if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).

7.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

(a) if the Relevant Authority is responsible for the relevant Personal Data Breach,

then the Relevant Authority shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Relevant Authority.

8. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (Joint Control Memorandum of Understanding), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 (Ending the contract).

9. Sub-Processing

9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

# Order Schedule 5 (Pricing Details)
# REDACTED

## Order Schedule 7 (Key Supplier Staff)

1.1 The Annex 1 to this Schedule lists the key roles ("Key Roles") and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.

1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.

1.3 The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.

1.4 The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:

1.4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);

1.4.2 the person concerned resigns, retires or dies or is on maternity or longterm sick leave; or

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

1.5 The Supplier shall:

1.5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);

1.5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;

1.5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff's employment contract, this will mean at least [ ] Months' notice;

1.5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables; and

1.5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced.

1.6 The Buyer may require the Supplier to remove or procure that any

Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

Annex 1 – Key Roles

| Key Role | Key Staff | Contact Details |
|---|---|---|
| Delivery Lead | REDACTED | REDACTED |
| Audit Manager | REDACTED | REDACTED |
| | | |
| | | |
| | | |

# Order Schedule 14 (Service Levels)

1. Definitions

1.1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

| | |
|---|---|
| "Critical Service Failure" | Means a failure to meet a Service Level Threshold in respect of a Service Level |
| "Service Credits" | any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels; |
| "Service Credit Cap" | has the meaning given to it in the Order Form; |
| "Service Level Failure" | means a failure to meet the Service Level Performance Measure in respect of a Service Level; |
| "Service Level Performance Measure" | shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and |
| "Service Level Threshold" | shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule. |

2. What happens if you don't meet the Service Levels

2.1. The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.

2.2. The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A of this Schedule including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to meet any Service Level Performance Measure.

2.3. The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.

2.4. A Service Credit shall be the Buyer's exclusive financial remedy for a Service Level Failure except where:

2.4.1. the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or

2.4.2. the Service Level Failure:

(a) exceeds the relevant Service Level Threshold;

(b) has arisen due to a Prohibited Act or wilful Default by the Supplier;

(c) results in the corruption or loss of any Government Data; and/or
(d) results in the Buyer being required to make a compensation payment to one or more third parties; and/or

2.4.3. the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).

3. Critical Service Level Failure
On the occurrence of a Critical Service Level Failure:

3.1. any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and
3.2. the Buyer shall (subject to the Service Credit Cap) be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period ("Compensation for Critical Service Level Failure"),
provided that the operation of this paragraph Error! Reference source not found. shall be without prejudice to the right of the Buyer to terminate this Contract and/or to claim damages from the Supplier for material Default.

## Part A: Service Levels and Service Credits

1. Service Levels
If the level of performance of the Supplier:

1.1 is likely to or fails to meet any Service Level Performance Measure;
1.2 is likely to cause or causes a Critical Service Failure to occur, the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:

1.2.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;
1.2.2 instruct the Supplier to comply with the Rectification Plan Process;
1.2.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or
1.2.4 if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure (including the right to terminate for material Default).

2. Service Credits

2.1 The Buyer shall use the Performance Monitoring Reports supplied by the Supplier to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.

2.2 Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in the Annex to Part A of this Schedule.

## Part B: Performance Monitoring

3. Performance Monitoring and Performance Review

3.1 Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.

3.2 The Supplier shall provide the Buyer with performance monitoring reports ("Performance Monitoring Reports") in accordance with the process and timescales agreed pursuant to paragraph Error! Reference source not found. of Part B of this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

3.2.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;

3.2.2 summary of all failures to achieve Service Levels that occurred during that Service Period;

3.2.3 details of any Critical Service Level Failures;

3.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;

3.2.5 the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and

3.2.6 such other details as the Buyer may reasonably require from time to time.

3.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("Performance Review Meetings") on a Monthly basis. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:

3.4 take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location and time (within normal business hours) as the Buyer shall reasonably require;

3.4.1 be attended by the Supplier's Representative and the Buyer's Representative; and

3.4.2 be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Buyer's Representative and any other recipients agreed at the relevant meeting.

3.5 The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Supplier's Representative and the Buyer's Representative at each meeting.

3.6 The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

4. Satisfaction Surveys

4.1 The Buyer may undertake satisfaction surveys in respect of the Supplier's provision of the Deliverables. The Buyer shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Deliverables which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.

# DPS Schedule 1 (Specification)

This Schedule sets out what we and our buyers want.
The Supplier must only provide the Deliverables for the Filter Categories that they have been appointed to.

For all Filter Categories and/or Deliverables, the Supplier must help Buyers comply with any specific applicable Standards of the Buyer.

The Deliverables and any Standards set out below may be refined (to the extent permitted and set out in the Order Form) by a Buyer during an Order Procedure to reflect its Deliverables Requirements for entering a particular Order Contract.

**Filter Category Level 1 – Services**

1 Quality Assurance Testing (QAT) Specialists
The Supplier shall provide access to a flexible and cost-effective pool of QA and Test professionals, who will form part of, and be managed by, the core Buyer's team to deliver services across the full lifecycle.

2 Quality Assurance (QA) & DevOps
The Supplier shall develop and implement test automation strategies and frameworks, typically to support cost effective continuous release methods. To support all aspects of software and platform engineering within a DevOps environment, from a QA perspective.

3 Load & Performance Testing
The Supplier shall identify, target and solve performance-based defects at any stage of the development lifecycle. The approach includes Load Testing, Stress Testing, Volume Testing, Soak Testing, Scalability Testing and Capacity Planning. Supporting performance engineering approaches where possible.

4 Quality Assurance (QA) & Testing
The Supplier shall establish and manage an appropriate level of QA and testing in line with programme delivery plans, validation and verification of a system against specifications and requirements covering functional and nonfunctional aspects. Testing will be automated by default with some requirement for manual, exploratory testing and assurance of testing owned by third-parties. Includes the ownership (design and execution) of complex, large scale integration testing.

5 Infrastructure Testing

The Supplier shall determine whether system infrastructures are performant, including network provisioning, platforms and hosting across LAN, WAN and Cloud infrastructures.

6 Operational Acceptance Testing (OAT)
The Supplier shall help prepare for operational readiness once the Service goes into production. OAT will generally focus on risks to the Service covering monitoring and alerting, IT support, failover, recovery, resilience, portability and stability.

7 Strategic Quality Assurance Consultancy
The Supplier shall provide strategic consultancy support across any aspect of QA across software and infrastructure engineering and broader Digital Data and Technology (DDaT) delivery as appropriate.

8 Accessibility Quality Assurance (QA) and Testing
The Supplier shall assess how far a product or Service is easy for its intended audience to use. That audience includes users who access the Service via a range of assistive technologies like screen readers, voice recognition and input devices. This includes helping the wider QA or product team to understand accessibility of the Service through expert consultancy.

9 Security Quality Assurance (QA) and Testing
The Supplier shall identify threats and measure potential vulnerabilities. The testing scope includes the whole system and not just the software involved. Much of the testing will be automated, supported by advanced exploratory testing and cyber-related defence and assessments.

10 Quality Assurance (QA) Capability Development
The Supplier shall provide support for all aspects of growing civil servant capability within the QA specialism including learning and development, recruitment, knowledge management and graduate/apprentice onboarding.

# DPS Schedule 3 (DPS Pricing)

1. How DPS Pricing is used to limit Order Charges

1.1. DPS Pricing:

1.1.1. will be used as the basis for capping the Charges by setting a maximum price for any Supplier Staff member offered to fulfil a Role that is the subject of an Order Contract.

1.1.2. The maximum price that can be tendered for any Supplier Staff member to fulfil a Role is £1000 per day (excluding VAT); and cannot be increased except as in accordance with this Schedule.

Note: The maximum day rate is in respect of a Professional Working Day ~~a~~ Working Day of no fixed length and being as long as to permit all scheduled work to be completed. Usually an eight-hour day unless agreed otherwise, but it means that the Supplier will not be paid overtime if it is longer than eight hours.

1.2. The Charges:

1.2.1. shall be calculated in accordance with the terms of the Order Contract and in particular in accordance with the terms of the Order Form;

1.2.2. cannot be increased except as specifically permitted by the Order Contract and subject to the maximum DPS Pricing set out in this Schedule and in particular shall only be subject to Indexation where specifically stated in the Order Form.

Note: Day rate-based Charges for all Order Contracts shall be calculated on the basis of Professional Working Days worked by Supplier Staff in the relevant Roles.

2. All costs and expenses are included in the Charges

2.1. Except as expressly set out in Paragraph 3 below, or otherwise stated in an Order Form the Charges shall include all costs and expenses relating to the provision of Deliverables. No further amounts shall be payable in respect of matters such as:

2.1.1. incidental expenses such as travel, subsistence and lodging, document or report reproduction, shipping, desktop or office equipment costs, network or data interchange costs or other telecommunications charges; or

2.1.2. costs incurred prior to the commencement of any Order Contract.

3. When the Supplier will be reimbursed for travel and subsistence

3.1. Expenses shall only be recoverable where:

3.1.1. a time and materials pricing mechanism is used; and

3.1.2. the Order Form states that recovery is permitted; and
3.1.3. they are Reimburseable Expenses incurred in line with the published departmental policy on travel & expenses and are supported by Supporting Documentation.

3.2.The Buyer shall provide a copy of their current expenses policy to the Supplier upon request.

4. When the DPS Pricing may change

4.1. The DPS Pricing, ie the £1000 per day maximum, will be fixed for the first three years following the DPS Contract Commencement Date (the date of expiry of such period is a "Review Date"). After this DPS Pricing can only be adjusted on each following yearly anniversary (the date of each such anniversary is also a "Review Date").
4.2.Subject to giving CCS at least three (3) Months' notice prior to the relevant Review Date the Supplier may recommend an increase in the permitted maximum.
4.3. Any notice recommending an increase shall include:
4.3.1. written evidence of the justification for the requested increase including:
a) details of the movement in the different cost components of the pricing in relation to the affected Role(s)
b) reasons for the movement in the different identified cost components of the relevant pricing
c) a breakdown of the profit and cost components that comprise the relevant pricing of the affected Role(s);
d) evidence that the Supplier has attempted to mitigate against the increase in the relevant cost components; and
e) evidence that the proportion of the pricing for the relevant Role(s) attributable to the Supplier's profit component is no greater than was typically the case at the DPS Start Date.

4.4. CCS shall consider the recommendations, along with any recommendations from other DPS suppliers, and may grant Approval to an increase at its sole discretion.
4.5. Where CCS approves an increase then it will be implemented from the first (1st) Working Day following the relevant Review Date or such later date as CCS may determine at its sole discretion.

5. Other events that may result in a change the DPS Pricing
5.1. The DPS Pricing can also be varied (and Annex 1 will be updated

accordingly) due to:

5.1.1. a Specific Change in Law in accordance with Clause 24;

5.1.2. a review in accordance with insurance requirements in Clause 13.

# Annex 1 – Quality Response

## Question 4.1: Supplier Experience

**Please provide 2 examples of your organisation's experience of delivering similar projects**

REDACTED

## Question 4.2: Resourcing the contract

**A plan of the proposed team including clear lines of reporting and the role each individual will have**

REDACTED

**Resource plans that clearly indicates the days spent on each activity per individual, with supporting rationale**

REDACTED

- 

**Evidence that your team are Suitably Qualified and Experienced Persons and have the necessary skills;**

REDACTED

**Why team members have been chosen for this Contract and what added value they could bring.**

REDACTED

## Question 5.1: Project management and governance

### Outline your approach and methodology for this project

REDACTED

Demonstrate your understanding of the standards WCAG 2.1 AA Regulations that are being tested

REDACTED

**How you would ensure all of the SLAs are met, as stated at paragraph 15.1 of the Statement of Requirements**

REDACTED

**Evidence for how you will maintain frequent contact with the Authority. This may include details of the proposed online tools to use**

REDACTED

**Evidence of the internal procedures for quality assurance and controls that are in place**

REDACTED

**Details for secure transfer of reports;**

REDACTED

**A risk management plan detailing potential risks specific to the projects and the steps you would take to mitigate them, as well as a Contingency and disaster recovery plan;**

REDACTED

**A plan for ensuring that the project is delivered on budget.**
REDACTED.

## A robust escalation procedure

REDACTED