



G-Cloud 13 Call-Off Contract

This Call-Off Contract for the G-Cloud 13 Framework Agreement (RM1557.13) includes:

G-Cloud 13 Call-Off Contract

Part A: Order Form	2
Part B: Terms and conditions	11
Schedule 1: Services	35
Schedule 2: Call-Off Contract charges	36
Schedule 3: Collaboration agreement	37
Schedule 4: Alternative clauses	37
Schedule 5: Guarantee	37
Schedule 6: Glossary and interpretations	38
Schedule 7: UK GDPR Information	49

Part A: Order Form

Buyers must use this template order form as the basis for all Call-Off Contracts and must refrain from accepting a Supplier's prepopulated version unless it has been carefully checked against template drafting.

Platform service ID number	850243765466614
Call-Off Contract reference	Atamis C231570
Call-Off Contract title	NHS Digital Staff Passports Technical Supplier
Call-Off Contract description	Provision of technical support services to enable development of the NHS Digital Staff Passports.
Start date	11 th December 2023
Expiry date	30 th August 2024
Call-Off Contract value	The total value of this Call Off Contract is £1,990,000 (ex VAT)
Charging method	Fixed price
Purchase order number	TBC

This Order Form is issued under the G-Cloud 13 Framework Agreement (RM1557.13).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Services offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

From the Buyer	NHS England 1 st Floor, Quarry House, Quarry Hill, Leeds, West Yorkshire, LS2 7UE
To the Supplier	Sitekit Applications Limited 17-21 Ashford Road Maidstone ME14 5DA
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: Project Manager



For the Supplier:

Title: Sales Manager





Call-Off Contract term

Start date	This Call-Off Contract Starts on 11 th December 2023 and is valid for 9 months unless extended by the Buyer.
Ending (termination)	The notice period needed for Ending the Call-Off Contract is at least 30 Working Days from the date of written notice for undisputed sums or at least 30 days from the date of written notice for Ending without cause.
Extension period	Extensions if required will be progressed in-compliance with the applicable G-Cloud 13 Ts&Cs.

Buyer contractual details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

G-Cloud Lot	<p>This Call-Off Contract is for the provision of Services Under:</p> <ul style="list-style-type: none"> • Lot 3: Cloud support
G-Cloud Services required	<p>Provision of technical support services to enable development of the NHS Digital Staff Passports. This will include:</p> <ul style="list-style-type: none"> • Project management • Proxy product ownership (UCD and Technical) • UCD • Technical application development, including API development. • Development Operations (DevOps) • Quality assurance • Testing • 2nd and 3rd line support <p>Below Documents in Schedule 9 and Schedule 10:</p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  Sitekit - NHS Digital Staff Passport Technic </div> <div style="text-align: center;">  G-Cloud 13_NHS Digital Staff Passpor </div> </div>

Additional Services	N/A
Location	The Services will be performed at the Buyer's offices in England UK or from the Supplier's offices or approved remote locations (including home working with approved locations) in each case as reasonably agreed between all parties.
Quality Standards	The quality standards required for this Call-Off Contract will align to industry good practice.
Technical Standards:	The technical standards required for this Call-Off Contract will align to Good Industry Practice. As well as the applicable standards listed within the G-Cloud service offerings.
Service level agreement:	N/A
Onboarding	The team will arrange a kick off call with relevant stakeholders upon commencing the services.
Offboarding	On completion of the services, the team will hand over all assessment documentation, and remove any access to relevant NHS England systems from their devices.
Collaboration agreement	N/A
Limit on Parties' liability	<p>The annual total liability for Buyer Data defaults will not exceed 125% of the aggregate fees paid by the Client under the Agreement during the one-year period immediately prior to the date on which the claim arose under this Agreement.</p> <p>In addition, the Supplier will be liable for direct loss of or damage to the tangible property of the Client to the extent the same has been caused directly by the negligence of the Supplier, (or its employees or agents acting in the course of their employment or agency), provided that the Supplier's liability for any such loss or damage will be limited to the sum of £50,000 in aggregate</p>

Insurance	<p>The insurance(s) required will be:</p> <ul style="list-style-type: none"> • professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £10,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) • employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Buyer's responsibilities	<p>The Buyer is responsible for:</p> <ul style="list-style-type: none"> • Granting timely access to relevant systems and documentation on prior request • Providing a safe working environment for the Supplier staff if onsite • Provide timely access to any relevant personnel and information to the Supplier's team <p>The Supplier will not be deemed in breach of any service levels defined in this contract caused by the Buyer failing to meet any of the responsibilities listed above.</p>
Buyer's equipment	<p>The Supplier will supply laptops for their staff to use in delivery of the Services.</p>

Supplier's information

Subcontractors or partners	N/A
-----------------------------------	-----

Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

Payment method	The payment method for this 'fixed priced' Call-Off Contract will be via BACS
-----------------------	---

Payment profile	The payment profile for this contract is monthly in arrears; payment will be made on successful delivery of sprints, approved and signed-off as acceptable by the NHSE's Product Lead/Technical Product Owner
Invoice details	<p>The Supplier will issue electronic invoices in accordance with the payment profile above.</p> <p>The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.</p>
Who and where to send invoices to	<p>Invoices will be sent to NHS Shared Business Service either electronically via Tradeshift or by post to the following address:</p> <p>NHS England X24 Payables K005 Phoenix House Topcliffe Lane Wakefield F3 1WE</p> <p>Additional information about the NHS Shared Business Service can be found at their website here.</p> <p>Important changes effective 1 April 2023: NHS England » Important changes for all suppliers trading with NHS England (NHS Digital) and Health Education England – what you need to know</p>
Invoice information required	<p>All invoices must include:</p> <ul style="list-style-type: none"> • NHS Purchase Order reference. • Supplier project reference. • Invoice reference number.
Invoice frequency	Invoices will be sent to the Buyer in accordance with the payment profile as above.
Call-Off Contract value	The total value of this Call-Off Contract is £1,990,000 (ex VAT)

Call-Off Contract charges	Fixed price payment on satisfactory completion of specified deliverables as approved by the Authority's representative.
----------------------------------	---

Additional Buyer terms

Performance of the Service	The key performance indicators are defined below.		
	Key Performance	Metric	Measurement
	Project Governance	Timely and accurate highlight reports detailing status, progress against timeline, dependencies, risks, issues and tracking against budget.	<ul style="list-style-type: none"> Weekly reports
		Maintenance of roadmap and detailed workplan	<ul style="list-style-type: none"> Weekly / fortnightly updated workplan
		Participation at regular stand ups and update meetings with team leadership	<ul style="list-style-type: none"> Weekly attendance Preparedness for meeting Good input in update/discussions
		Attendance and presenting at regular governance meetings, including preparing papers in advance	<ul style="list-style-type: none"> Attendance, as required. Preparedness for meeting Quality of presentation materials
		Providing materials to aid senior decision-making	<ul style="list-style-type: none"> Availability for ad hoc requests Quality of material
	Stakeholder management	Attendance and presenting at key stakeholder meetings, including preparing papers in advance.	<ul style="list-style-type: none"> Weekly / monthly attendance Preparedness for meeting Good input in update/discussions Quality of materials
		Developing and maintaining relationships with key suppliers and stakeholders	<ul style="list-style-type: none"> Feedback from key suppliers and stakeholders on the good relationship
	Collaboration	Collaborative approach with suppliers and stakeholders to ensure co-design and sharing of expertise and knowledge	<ul style="list-style-type: none"> Evidence of participation in the network, and input and feedback regarding specs
	Effectiveness	Response to identified issues.	<ul style="list-style-type: none"> Time taken to respond to identified issues.
Guarantee	N/A		
Warranties, representations	N/A		
Supplemental requirements in addition to the Call-Off terms	N/A		

Alternative clauses	N/A
Buyer specific amendments to/refinements of the Call-Off Contract terms	N/A
Personal Data and Data Subjects	N/A
Intellectual Property	<p>The NHS Community Edition shall constitute Supplier-owned foreground IPR for the purposes of this contract. Condatis (through Sitekit) will provide the Authority with the source code for the NHS Community Edition of the Condatis Credential Gateway, on terms of the license below.</p> <p>The Supplier will provide the Condatis Credential Gateway to the NHS Commissioning Board (known as NHS England) on Software and the NHS Commissioning Board (Known as NHS England) shall not be entitled to use the source code and other deliverables of the NHS Community Edition, unless and until the licence is granted below.</p> <p>In the event that the Contract is terminated for failure to deliver, or material breach, or expires, and is not replaced by any similar contract for Condatis Credential Gateway or any similar product, the NHS Commissioning Board (Known as NHS England) shall be entitled to use the NHS Community Edition on the following terms:</p> <ul style="list-style-type: none"> • Non commercially exploitable • Non-transferable or sub-licensable • Non revokable • In perpetuity • Usable only by the Authority or successor organisations in England and only in the field of Health and Social Care. <p>For the avoidance of doubt, if the above licence is granted, the Supplier shall provide the Authority with the source code for the NHS Community Edition within 7 days to enable it to be make use of the license.</p>

Social Value	N/A
---------------------	-----

1. Formation of contract

- 1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a CallOff Contract with the Buyer.
- 1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.
- 1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.
- 1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

2. Background to the agreement

- 2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.13

Signed	Sitekit Applications Limited (The Supplier) Signed by:	NHS England (The Buyer)
Name		
Title	Job Title/Role: CEO Chief Executive Officer Date Signed: 2 January 2024	Job Title/Role: Director of Financial t Director of Financial Control Date Signed: 4 January 2024

2.2 The Buyer provided an Order Form for Services to the Supplier.

Customer Benefits
For each Call-Off Contract please complete a customer benefits record, by following this link:

[G-Cloud 13 Customer Benefit Record](#)

Part B: Terms and conditions

1. Call-Off Contract Start date and length

- 1.1 The Supplier must start providing the Services on the date specified in the Order Form.
- 1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 36 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.
- 1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.
- 1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 24 months.

2. Incorporation of terms

- 2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:
 - 2.3 (Warranties and representations)
 - 4.1 to 4.6 (Liability)
 - 4.10 to 4.11 (IR35)
 - 10 (Force majeure)
 - 5.3 (Continuing rights)
 - 5.4 to 5.6 (Change of control)
 - 5.7 (Fraud)
 - 5.8 (Notice of fraud)
 - 7 (Transparency and Audit)
 - 8.3 (Order of precedence)
 - 11 (Relationship)
 - 14 (Entire agreement)
 - 15 (Law and jurisdiction)
 - 16 (Legislative change)
 - 17 (Bribery and corruption)

- 18 (Freedom of Information Act)
- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)
- 24 (Conflicts of interest and ethical walls)

- 25 (Publicity and branding)

- 26 (Equality and diversity)
- 28 (Data protection)
- 31 (Severability)
- 32 and 33 (Managing disputes and Mediation)
- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

- 2.2.1 a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'
- 2.2.2 a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'
- 2.2.3 a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

- 2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 7 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

- 2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'XX', where 'XX' is the Framework Agreement clause number.

- 2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

3. Supply of services

- 3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.
- 3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

4. Supplier staff

- 4.1 The Supplier Staff must:
 - 4.1.1 be appropriately experienced, qualified and trained to supply the Services
 - 4.1.2 apply all due skill, care and diligence in faithfully performing those duties
 - 4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
 - 4.1.4 respond to any enquiries about the Services as soon as reasonably possible
 - 4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer
- 4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.
- 4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
- 4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.
- 4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.
- 4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14digit ESI

reference number from the summary outcome screen and promptly provide a copy to the Buyer.

- 4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.
- 4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

- 5.1 Both Parties agree that when entering into a Call-Off Contract they:
 - 5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
 - 5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms
 - 5.1.3 have raised all due diligence questions before signing the Call-Off Contract
 - 5.1.4 have entered into the Call-Off Contract relying on their own due diligence

6. Business continuity and disaster recovery

- 6.1 The Supplier will have a clear business continuity and disaster recovery plan in their Service Descriptions.
- 6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.
- 6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

- 7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.

- 7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
 - 7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.
 - 7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.
 - 7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.
 - 7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.
- 7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.
- 7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
 - 7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.
 - 7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any

undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.
 - 7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

- 7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

8. Recovery of sums due and right of set-off

- 8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

9. Insurance

- 9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

- 9.2 The Supplier will ensure that:

9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000

9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit

9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

- 9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

- 9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:
 - 9.4.1 a broker's verification of insurance
 - 9.4.2 receipts for the insurance premium
 - 9.4.3 evidence of payment of the latest premiums due
- 9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:
 - 9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
 - 9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances
 - 9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance
- 9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.
- 9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.
- 9.8 The Supplier will be liable for the payment of any:
 - 9.8.1 premiums, which it will pay promptly
 - 9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

- 10.1 The Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under incorporated Framework Agreement clause 34. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

11.1 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party

shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.

11.2 Neither Party shall have any right to use any of the other Party's names, logos or trade marks on any of its products or services without the other Party's prior written consent.

11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:

11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and

11.3.2 the Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer's written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.

11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

11.5 Subject to the limitation in Clause 24.3, the Buyer shall:

11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:

- (a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
- (b) alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;
- (c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and

11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgment against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer's obligations under this Clause 11.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier's breach of this Contract.

11.6 The Supplier will, on written demand, fully indemnify the Buyer for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:

11.6.1 rights granted to the Buyer under this Call-Off Contract

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

11.7 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

11.7.1 modify the relevant part of the Services without reducing its functionality or performance

11.7.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer

11.7.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.8 Clause 11.6 will not apply if the IPR Claim is from:

11.8.1 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract

11.8.2 other material provided by the Buyer necessary for the Services

11.9 If the Supplier does not comply with this clause 11, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

12.1.1 comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data

12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body

12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

12.2.1 providing the Buyer with full details of the complaint or request

12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions

12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject
(within the timescales required by the Buyer)

12.2.4 providing the Buyer with any information requested by the Data Subject

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

13. Buyer data

13.1 The Supplier must not remove any proprietary notices in the Buyer Data.

13.2 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.

13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

- 13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.
- 13.5 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.
- 13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

13.6.1 the principles in the Security Policy Framework:

<https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy: <https://www.gov.uk/government/publications/government-securityclassifications>

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management:

<https://www.cpni.gov.uk/content/adopt-risk-managementapproach> and Protection of Sensitive Information and Assets: <https://www.cpni.gov.uk/protection-sensitive-information-and-assets>

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance: <https://www.ncsc.gov.uk/collection/risk-management-collection>

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint: <https://www.gov.uk/government/publications/technologycode-of-practice/technology-code-of-practice>

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance: <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>

13.6.6 Buyer requirements in respect of AI ethical standards.

13.7 The Buyer will specify any security requirements for this project in the Order Form.

- 13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if

corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

- 13.9 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.
- 13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

- 14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.
- 14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at:
<https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
- 14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.
- 14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.
- 14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

- 15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.
- 15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

16. Security

- 16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.
- 16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
- 16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.
- 16.4 Responsibility for costs will be at the:
- 16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided
- 16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control
- 16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.
- 16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:
<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>
- 16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

17. Guarantee

17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:

17.1.1 an executed Guarantee in the form at Schedule 5

17.1.2 a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the

Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided

18.2.2 Call-Off Contract Charges paid during the notice period are reasonable compensation and cover all the Supplier's avoidable costs or Losses

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied

18.4.2 any fraud

18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so

18.5.2 an Insolvency Event of the other Party happens

18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

19.4.1 any rights, remedies or obligations accrued before its Ending or expiration

19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry

19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)

- 24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability),
24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

19.4.4 any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires.

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

- 19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
- 19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
- 19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer
- 19.5.4 destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law
- 19.5.5 work with the Buyer on any ongoing work
- 19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

20. Notices

20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.

- Manner of delivery: email
- Deemed time of delivery: 9am on the first Working Day after sending
- Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message

20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services

from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the period on terms that are commercially reasonable and acceptable to the Buyer

21.6.2 there will be no adverse impact on service continuity

21.6.3 there is no vendor lock-in to the Supplier's Service at exit

21.6.4 it enables the Buyer to meet its obligations under the Technology Code Of Practice

21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.

21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:

21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier

21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer

21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier

21.8.4 the testing and assurance strategy for exported Buyer Data

21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations

21.8.6 any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

22. Handover to replacement supplier

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control

22.1.2 other information reasonably requested by the Buyer

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than 30 consecutive days, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges

paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the

Supplier's liability:

24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited; and

24.2.2 in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.

24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the

Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).

24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause

24.2 will not be taken into consideration.

25. Premises

25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer's premises, the Supplier will:

25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises

25.5.2 comply with Buyer requirements for the conduct of personnel

25.5.3 comply with any health and safety measures implemented by the Buyer

25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

27. The Contracts (Rights of Third Parties) Act 1999

27.1 Except as specified in clause 29.8, a person who isn't Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

28. Environmental requirements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to

End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

- 29.2.1 the activities they perform
- 29.2.2 age
- 29.2.3 start date
- 29.2.4 place of work
- 29.2.5 notice period
- 29.2.6 redundancy payment entitlement
- 29.2.7 salary, benefits and pension entitlements
- 29.2.8 employment status
- 29.2.9 identity of employer
- 29.2.10 working arrangements
- 29. 2.11 outstanding liabilities
- 29.2.12 sickness absence
- 29.2.13 copies of all relevant employment contracts and related documents
- 29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

29.3 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

29.4 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.

29.5 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:

29.5.1 its failure to comply with the provisions of this clause

29.5.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

29.6 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

29.7 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause, but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.

31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:

31.2.1 work proactively and in good faith with each of the Buyer's contractors

31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

- 32.1 The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.
- 32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.
- 32.3 If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this CallOff Contract by giving 30 days notice to the Supplier.

33. Data Protection Legislation (GDPR)

- 33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7.

Schedule 1: Services

1. Aim:

- 1.1 The NHS Digital Staff Passport (DSP) is currently in private beta development. NHS England are looking to award an interim contract for a technical supplier to run from 11th December 2023 to 30 August 2024. The interim contract will ensure the DSP is stable enough to roll out the private beta and gather detailed requirements for the public beta.
- 1.2 The purpose of this document is to provide a brief to shortlisted suppliers of our requirements to enable them to determine whether they can meet our specifications, match our services and that they have the capacity and availability for call-off and to clarify how they will deliver the specified requirements within the allocated time and capped budget envelope.
- 1.3 The capped budget envelope for this requirement is £2,000,000 (excluding VAT)

2. Background:

- 2.1 The NHS has committed in the [Long Term Plan](#) to enable “staff to move more easily from one NHS Employer to the other”. This was emphasised in the Interim People Plan and re-emphasised in subsequent versions. The [2023/24 NHS operational planning guidance](#) also speaks to the need for flexible workforce deployment of staff across organisational boundaries using digital solutions such as the Digital Staff Passport. The long awaited [Long Term Workforce Plan](#) now expects the full roll out of the Digital Staff Passport by August 2025. This procurement is therefore critical to the delivery of a key NHS ambition to enable staff to move.
- 2.2 **The NHS Digital Staff Passport (DSP)** is a trusted and secure digital means by which NHS employees can digitally transfer their key employment data between different NHS employers and into their respective workforce systems. The DSP facilitates an adaptable and agile workforce who can move seamlessly between NHS Trusts in a way that safeguard services and patients.
- 2.3 To enable rapid deployment of key workers in support of the NHS response to COVID-19, the DSP development was accelerated. This led to the interim COVID-19 DSP, a solution that enabled securely sharing a point-in-time snapshot of a staff member’s employment status, so that the worker does not need to repeat employment checks when they were temporarily deployed in response to the COVID-19 pandemic. The evolution of this interim COVID-19 DSP is the new NHS DSP, which will enable secure transfer of key staff employment check information.

3. Requirements:

3.1 Functions required for NHS organisation portals and credential gateway.

- Project management
- Proxy product ownership (UCD and Technical)
- UCD
- Technical application development, including API development.
- Development Operations (DevOps)
- Quality assurance
- Testing
- 2nd and 3rd line support

3.2 Functional deliverables required.

- New and enhanced requirements after Minimum Viable Product (MVP) release for the DSP service covering both the NHS organisations' portals and the credential gateway.
- Project management / Product Owners
 - Collaborative working with the Authority's Project managers / Delivery Lead to co-ordinate different suppliers, meetings, follow-up meeting notes etc.
 - Weekly Programme Board reporting
 - Sprint ceremonies – sprint planning, sprint demonstrations, sprint retrospectives
 - Leading elaboration sessions on business requirements
- Backlog / sprint management
 - Requirements/Stories and Acceptance Criteria captured in DevOps – refined through initial requirements from the Authority's product lead, elaboration sessions, approved UCD and detailed acceptance criteria for developers/testers before the commencement of development work.
 - Estimates for Requirements/Stories (in Story Points) within DevOps
 - Running sprint planning, demo and retros for UCD and development teams that includes the Authority's product lead / technical product owner to ensure stories are fully understood, prioritisations are clear.
 - ❖ *The Authority's Product Lead and Technical Product Owner will make all prioritisation decisions for the sprint and will require their approval to move stories from one sprint to the next.*
 - Daily stand ups.
- Solution architecture.

- Elaboration, validation and sign off requirements within joint elaboration sessions. Attended as a minimum by the supplier product owner, lead architect and developer.
 - ❖ the Authority's Product lead and technical product owner to be involved in these elaboration sessions with the supplier development team to ensure requirements are fully understood before planning and development starts.
- Update of technical documentation, where relevant.
- UCD.
 - Elaboration, validation and sign off requirements within joint elaboration sessions. Attended as a minimum by supplier product owner, lead architect and developer.
 - Live design sessions for features that require collective sign off.
 - Design documentation kept up to date with relevant details for testing team.
 - UCD following NHS Service Manual, W3C accessibility standards, content consistency.
- Development.
 - Elaboration, validation and sign off requirements within joint elaboration sessions. Attended as a minimum by the supplier product owner, lead architect and developer.
 - ❖ the Authority's product lead and technical product owner to be involved in these elaboration sessions with the supplier development team to ensure requirements are fully understood before planning and development starts.
 - Update of technical documentation, where relevant.
- QA / Testing.
 - Sprint planning to ensure acceptance criteria is clearly defined ahead of start of development.
 - Test scripts.
 - Release notes.
 - Regression testing
 - ❖ Ensuring no new defects are introduced with defect fixes and new features.
 - Defect management process.
- DevOps.
 - Optimisation of deployment process.
 - Maintenance of deployment process documentation / installation guide.
- 2nd and 3rd line support
 - Service commitments as outlined in table below.

- Options for dedicated support team to incidents triaging and fixing can be prioritised into a sprint, with acknowledgement that P1 and P2 issues may disrupt the ongoing sprint and P3-P5 issues will need to be triaged before being planned in.
- Completion and communication of Service Request, Incident or Problem Resolution

Operational hours (service hours)	24x7x365
Business support hours (service support hours)	8 – 6pm Monday to Friday (excluding Bank Holidays)
Availability (in business support hours)	99.5% (with an aim to move to 99.9%)
Incident resolution times (in business support hours)	
Severity 1	4 hours
Severity 2	8 hours
Severity 3	20 hours
Severity 4	80 hours
Problem fix times	
Severity 1	30 working days or an agreed release
Severity 2	60 working days or an agreed release
Severity 3	120 working days or an agreed release
Severity 4	240 working days or an agreed release
Service reporting	Monthly
Disaster recovery	4 hours
Recovery point objective (RPO)	24 hours

3.3 Process required:

3.3.1 The Authority requires sprints of 2-weeks duration (10 working days) of the following size (in story points) for:

- UCD: 15- 25 story points per sprint.
- Application development: 75 – 85 story points per sprint
- Supplier to work closely with the Authority's product lead / technical product owner to review assigned story points within sprint planning sessions.

- Supplier to apply Fibonacci sequencing to ascertain story points (1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144)
- DSP product backlog requirements which extend beyond the 75 to 85 story points for a sprint will be organised as Epics, Features and then Stories to breakdown the story points for the requirement. This means stories can be completed within one sprint, whilst the overall epic / feature will then be delivered across multiple sprints.
- 2nd and 3rd line support queries to be prioritised into the sprint as their occur. P1, P2 issues may disrupt an ongoing sprint, P3-P5 issues to be planned in.

3.3.2. The Authority will manage the releases for Production deployments with support from the supplier. The supplier's requirement is for:

- All features and functionality to be tested and signed off within UAT environment and preparing deployment packages for other environments (training, pre-production, production).
- The supplier to ensure a branching strategy is adhered to ensure product backlog functionality development is managed within lower environments and can be deployed into UAT environments for testing.
- The supplier to work closely with the Authority's release manager to ensure only approved product backlog features are deployed into the relevant environment.

3.3.3. The Authority requires best practice governance of sprint / release approval process. The following sprint approval checklist agreed at a minimum agreed and in place before each discrete sprint starts:

- **Sprint goal:** this is the overarching objective that the team is trying to achieve for the sprint.
- **Backlog items:** these are the specific tasks that need to be completed in order to achieve the sprint goal.
- **Definition of Done:** this is a list of criteria that must be met for a backlog item to be considered complete.
- **Acceptance criteria:** these are the specific requirements that must be met for a backlog item to be accepted by the product owner.
- **Sprint tasks:** these are the smaller tasks that need to be completed in order to complete a backlog item.
- **Sprint burndown chart:** this chart tracks the team's progress towards completing the sprint backlog.
- **Sprint review:** this meeting is held at the end of the sprint to demonstrate the work that has been completed.

- **Sprint retrospective:** this meeting is held at the end of the sprint to discuss what went well, what could be improved, and how the team can work more effectively in the next sprint.
 - Visibility of the supplier's internal retrospectives to feed into monthly sprint retrospective with the Authority.
- **Impediments:** these are any roadblocks or challenges that are preventing the team from completing the sprint backlog.
- **Documentation:** this includes any documentation that was created during the sprint, such as user stories, wireframes, or code comments.
- **Testing:** this ensures that the work that was completed in the sprint meets the quality standards.
- **Deployment:** this is the process of making the work that was completed in the sprint available to users.

3.3.4. The Authority requires the following to be documented and agreed to have taken place before a release is approved.

- **Project name, team and client:** this information helps to identify the release and the people involved.
- **Release number and date:** this information helps to track the release and ensure that it is properly scheduled.
- **Release goals and objectives:** this information helps to ensure that the release is aligned with the project's overall goals.
- **Requirements:** this information ensures that the release meets the needs of the users.
- **Dependencies:** this information identifies any other releases or systems that the release depends on.
- **Testing:** this information ensures that the release is tested and ready for deployment.
- **Deployment plan:** this information describes how the release will be deployed to production.
- **Rollback plan:** this information describes how to roll back the release if necessary.
- **Communication plan:** this information describes how the release will be communicated to the users.
- **Documentation:** this information provides documentation for the release, such as user guides and release notes.
- **Approvals:** This information ensures that the release has been approved by all stakeholders.

- **Post-release activities:** This information describes the activities that will be performed after the release, such as monitoring and maintenance.

3.3.5. The Authority requires best practice format for sprint demonstration and retrospective. Agenda as follows.

- **Sprint demonstration agenda**

- **Completed work:** the team should demonstrate the work that they have completed during the sprint. This could include new features, bug fixes, or improvements to existing functionality.
- **Acceptance criteria:** the team should demonstrate that the work meets the acceptance criteria that was agreed upon with the product owner.
- **User stories:** the team should explain the user stories that were implemented during the sprint. This helps to ensure that the work is aligned with the needs of the users.
- **Questions and feedback:** the team should be open to questions and feedback from the product owner, stakeholders, and other team members. This helps to ensure that the work meets the expectations of everyone involved.
- **Next steps:** the team should discuss the next steps for the product. This could include planning the next sprint, releasing the work to production, or gathering more feedback from users.

- **Sprint retrospective agenda**

- **What went well?** this is an opportunity for the team to celebrate its successes and learn from them.
- **What could be improved?** this is where the team can identify areas for improvement and make plans to address them.
- **What will we commit to improving in the next sprint?** this is where the team makes specific commitments to improve their processes and results.
- **Review of Story Point Estimates:** report on accuracy of estimates +/- and actions to improve. Identification of areas of trends.
- **Action items:** the team should come up with specific actions that they will take to address the areas for improvement. These actions should be assigned to specific people and have due dates.
- **Follow-up:** the team should schedule a follow-up meeting to discuss the progress of the action items.
- **Continual Service Improvement (CSI) Sprint Retrospective Questions:**
 - ❖ What were the biggest challenges we faced?

- ❖ How can we communicate better with each other?
- ❖ How can we make our work environment more efficient?
- ❖ How can we improve our testing process?
- ❖ How can we get better feedback from users?
- ❖ What are our goals for the next sprint?
- ❖ What are the risks and challenges we need to be aware of?

4. Target Outcomes:

High level roadmap for post MVP release is outlined below which is planned to be one release per month – to be confirmed with the Authority. The target outcome for this contract is as follows:

- Release 8 / 9 – January 2024
- Release 9 / 10 – February 2024
- Release 10/ 11 – March 2024 (scope to be confirmed based on private beta feedback)
- Release 12 – April 2024 (scope to be confirmed based on private beta feedback)
- Release 13 – May 2024 (scope to be confirmed based on private beta feedback)
- Release 14 – June 2024 (scope to be confirmed based on private beta feedback)
- Release 15 – July 2024 (scope to be confirmed based on private beta feedback)
- Release 16 – August 2024 (scope to be confirmed based on private beta feedback)

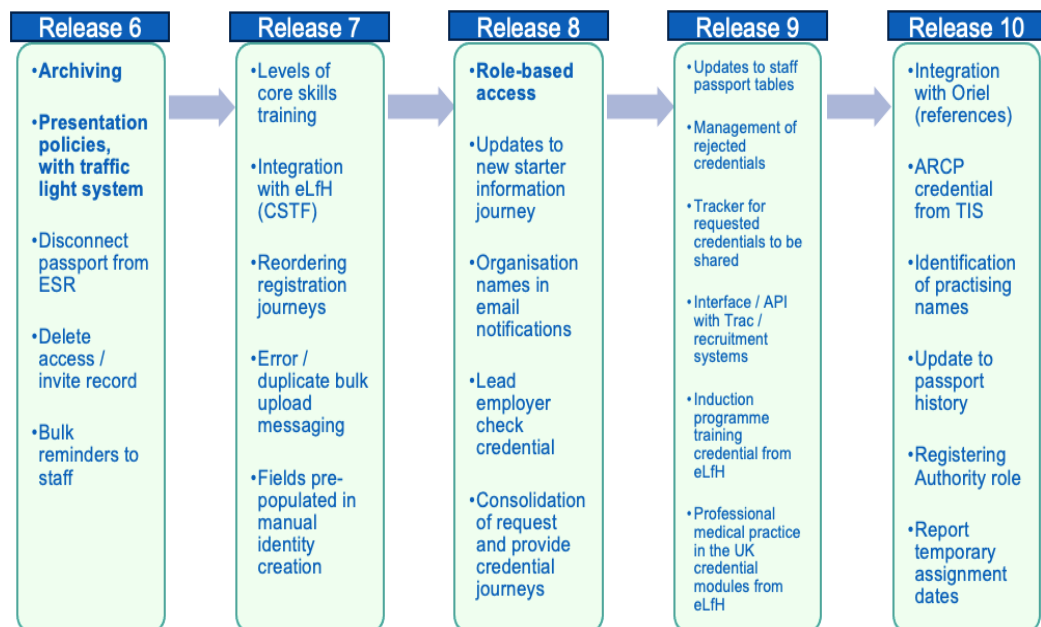


Figure 1: High level release plan

Reprioritisation of features in each release on approval of the Authority's product lead / technical product owner only.

Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Platform pricing document) can't be amended during the term of the Call-Off Contract.

The detailed Charges breakdown for the provision of Services during the Term will include:

Sprints	Start	Finish	Payment Milestones	Month	Net	VAT	Total Amount Payable
Condatix Gateway	01/01/2024	31/08/2024	Condatix gateway licence payment	December			
Sprint 37,38 and 39	11/12/2023	29/12/2023	Successful delivery of Sprints 37, 38 and 39	December			
Sprint 40	01/01/2024	12/01/2024	Successful delivery of Sprints 40 and 41	January			
Sprint 41	15/01/2024	26/01/2024					
Sprint 42	29/01/2024	09/02/2024	Successful delivery of Sprints 42 and 43	February			
Sprint 43	12/02/2024	23/02/2024					
Sprint 44	26/02/2024	08/03/2024	Successful delivery of Sprints 44 and 45	March			
Sprint 45	11/03/2024	22/03/2024					
Sprint 46	25/03/2024	05/04/2024	Successful delivery of Sprints 45, 46 and 47	April			
Sprint 47	08/04/2024	19/04/2024					
Sprint 48	22/04/2024	03/05/2024	Successful delivery of Sprints 49 and 50	May			
Sprint 49	06/05/2024	17/05/2024					
Sprint 50	20/05/2024	31/05/2024	Successful delivery of Sprints 51 and 52	June			
Sprint 51	03/06/2024	14/06/2024					
Sprint 52	17/06/2024	28/06/2024	Successful delivery of Sprints 53 and 54	July			
Sprint 53	01/07/2024	12/07/2024					
Sprint 54	15/07/2024	26/07/2024	Successful delivery of Sprints 55, 56 and 57	August			
Sprint 55	29/07/2024	09/08/2024					
Sprint 56	12/08/2024	23/08/2024					
Sprint 57	26/08/2024	30/08/2024					
Totals					£1,991,586.13	£398,317.23	£2,389,903.35
PO cost					£1,990,000.00	£398,000.00	£2,388,000.00

Schedule 3: Collaboration Agreement

Not used.

Schedule 4: Alternative Clauses

Not used.

Schedule 5: Guarantee

Not used.

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform).
Audit	An audit carried out under the incorporated Framework Agreement clauses.
Background IPRs	<p>For each Party, IPRs:</p> <ul style="list-style-type: none"> owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes created by the Party independently of this Call-Off Contract, or <p>For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.</p>
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.

Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	<p>Data, Personal Data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none"> information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the UK GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.

Data Protection Legislation (DPL)	(i) the UK GDPR as amended from time to time; (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.
Data Subject	Takes the meaning given in the UK GDPR
Default	<p>Default is any:</p> <ul style="list-style-type: none"> • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract <p>Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.</p>
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE')
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	<p>The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here:</p> <p>https://www.gov.uk/guidance/check-employment-status-for-tax</p>

Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force <p>Majeure at the time this Call-Off Contract was entered into</p> <ul style="list-style-type: none"> • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.13 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown

Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.

Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	Can be: <ul style="list-style-type: none"> • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium • a Dun & Bradstreet rating of 10 or less
Intellectual Property Rights or IPR	Intellectual Property Rights are: <ul style="list-style-type: none"> • copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information • applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction • all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: <ul style="list-style-type: none"> • the supplier's own limited company • a service or a personal service company • a partnership <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>
IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or Buyer's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' Losses ' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement Schedule 6.
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.

Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the UK GDPR.
Personal Data Breach	Takes the meaning given in the UK GDPR.
Platform	The government marketplace where Services are available for Buyers to buy.
Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK GDPR.

Prohibited act	<p>To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:</p> <ul style="list-style-type: none"> • induce that person to perform improperly a relevant function or activity • reward that person for improper performance of a relevant function or activity • commit any offence: <ul style="list-style-type: none"> ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation 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 such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's highperformance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.

Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service data	Data that is owned or managed by the Buyer and used for the GCloud Services, including backup data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controlscheck-if-you-need-approval-to-spend-money-on-a-service

Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the GCloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract. Schedule 8: DPA
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7: GDPR

Schedule 8: Data Processing Agreement (DPA)

DATA PROCESSING AGREEMENT (DPA)

between

(1) NHS England

and

(2) Sitekit Applications Ltd

CONTENTS

CLAUSE	PAGE
1 DEFINITIONS AND INTERPRETATION	1
2 SCOPE OF THIS AGREEMENT	4
3 PROCESSING OF PERSONAL DATA	5
4 INTERNATIONAL PERSONAL DATA TRANSFERS	12
5 TERM AND TERMINATION	13
6 REMEDIES AND NO WAIVER	14
7 NOTICES	14
8 GENERAL	15
9 GOVERNING LAW AND JURISDICTION	15
10 REVIEWERS	16
11 SIGNATORIES	17
12 APPENDIX 1 – DATA PROCESSING SERVICES	18
13 APPENDIX 2 - BACKGROUND	21

Personal Data Processing Review (PDPR) or Data Protection Impact Assessment (DPIA)

DPIA IG2023069 Approved

THIS AGREEMENT is made on

BETWEEN:

- (1) NHS England of Quarry House, Leeds, LS2 7UE (**NHS England**); and
- (2) Sitekit Applications Ltd (Company number 08194698) with its registered office at 17-21 Ashford Road, Maidstone, England, ME14 5DA (**Supplier**).

IT IS AGREED as follows:

1 DEFINITIONS AND INTERPRETATION

- 1.1 The following definitions shall apply in this Agreement:

Controller shall take the meaning given in the Data Protection Legislation;

Data Guidance means any applicable guidance, guidelines, direction or determination, framework, code of practice, standard or requirement regarding information governance, confidentiality, privacy or compliance with the Data Protection Legislation (whether specifically mentioned in this Agreement or not) to the extent published and publicly available or their existence or contents have been notified to the Supplier by NHS England and/or any relevant Regulatory or Supervisory Body. This includes but is not limited to guidance issued by NHS England (including applicable guidance published by NHS Digital prior to its merger with NHS England on 1 February 2023, the National Data Guardian for Health & Care, the Department of Health and Social Care, the Health Research Authority, and the Information Commissioner;

Data Loss Event means any event that results, or may result, in unauthorised Processing of Personal Data held by the Supplier under this Agreement or Personal Data that the Supplier has responsibility for under this Agreement including without limitation actual or potential loss, destruction, corruption or inaccessibility of Personal Data, including any Personal Data Breach;

Data Processing Services means the data processing services described in Appendix 1 of this Agreement;

Data Protection Impact Assessment means an assessment of the impact of the envisaged Processing on the protection of Personal Data;

Data Protection Legislation means UK Data Protection legislation currently comprising of (i) the DPA 2018 (ii) the UK GDPR, (iii) the Law Enforcement Directive and all applicable Law concerning privacy, confidentiality or the processing of personal data including but not limited to the Human Rights Act 1998, the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications) Regulations (PECR);

Data Protection Officer shall take the meaning given in the Data Protection Legislation;

Data Subject shall take the meaning given in the Data Protection Legislation;

Data Subject Access Request means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;

DPA 2018 means Data Protection Act 2018;

EEA Means European Economic Area;

EU means the European Union;

EU GDPR means the EU General Data Protection Regulation (Regulation (EU) 2016/679);

Information Commissioner means the independent authority established to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals (www.ico.org.uk) and any other relevant data protection or supervisory authority recognised pursuant to the Data Protection legislation;

Law means any law or subordinate legislation within the meaning of Section 21(1) of the UK Interpretation Act 1978.

LED means Part 3 of the Data Protection Act 2018 that brought the EU Law Enforcement Directive EU2016/680 into UK law.

Personal Data shall take the meaning given in the Data Protection Legislation;

Personal Data Breach shall take the meaning given in the Data Protection Legislation;

Processor shall take the meaning given in the Data Protection Legislation;

Processing and cognate terms shall have the meaning given in the Data Protection Legislation;

Protective Measures means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data; ensuring confidentiality, integrity, availability and resilience of systems and services; ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident; and regularly assessing and evaluating the effectiveness of such measures;

Regulatory or Supervisory Body means any statutory or other body having authority to issue guidance, standards or recommendations with which the Supplier and/or Supplier Personnel must comply or to which it or they must have regard, including:

- CQC;
- NHS England;
- the Department of Health and Social Care;
- the National Institute for Health and Care Excellence;
- Healthwatch England and Local Healthwatch;
- the General Pharmaceutical Council;
- the Healthcare Safety Investigation Branch;
- Information Commissioner;

Services means the goods and/or services to be supplied by the Supplier under the Supply Agreement;

Supplier Sub-processor means any third party Processor appointed to process Personal Data on behalf of the Supplier related to this Agreement;

International Data Transfer Agreement (IDTA) means the international data transfer agreement (IDTA) for the transfer of Personal Data from a Data Controller in the UK or a country defined as adequate by the UK Secretary of State under section 17A (general processing) or section 74A (law enforcement processing) of the UK Data Protection Act 2018 (DPA) to processors established in third countries or any alternative or successor decisions by the Secretary of State that approves

new standard contractual clauses for transfers to Data Processors in third countries), located [here](#).

Sub-processor shall take the meaning given in the Data Protection Legislation;

Supplier Personnel means any and all persons employed or engaged from time to time in the provision of the Services and/or the Processing of Personal Data whether employees, workers, consultants or agents of the Supplier or any subcontractor or agent of the Supplier.;

UK GDPR means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018, together with the Data Protection Act 2018, the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and other data protection or privacy legislation in force from time to time in the United Kingdom.

Working Day means a day other than a Saturday, Sunday or bank holiday in England.

- 1.2 reference to any legislative provision shall be deemed to include any statutory instrument, by-law, regulation, rule, subordinate or delegated legislation or order and any rules and regulations which are made under it, and any subsequent re-enactment, amendment or replacement of the same;
- 1.3 the Annex forms part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annex; and
- 1.4 references to clauses, appendices and annexes are to clauses and annexes to this Agreement.

2 SCOPE OF THIS AGREEMENT

- 2.1 The Digital Staff Passport solution contains the Employer's and Employee's portal. The Supplier will supply the means to deploy the solution and has tested this (automated) mechanism with NHS England Corporate IT in a testing environment. The plan is for NHS England Corporate IT to manage the live deployments.
 - 2.1.1 The solution also contains a Credential Gateway component. The Credential Gateway is offered as a separate SaaS (Software as a service) component, of which the Supplier will be the primary data processor of. The Supplier is granted the right in this Agreement to delegate the Credential Gateway Processing to Condatis Group Ltd, a Supplier Sub-processor and partner company, (hereinafter referred to as "Condatis"), via a sub-processing agreement. An additional solution

component, the digital wallet, is not under the scope of the Supplier or Condatis.

- 2.1.2 The Digital Staff Passport (Employee and Employer portals and associated backend components) are to be deployed to an NHS England controlled Microsoft Azure tenant. The Supplier will be granted some level of access to these components in production, for the purposes of ad hoc deployment and 3rd line managed service support.
- 2.2 The audit database will contain logged data different actions for the different credentials and events, completed by different user types e.g., PGD (Post Graduate Doctors), temporary staff, HR or other authorised users are logged. NHSE will extract transform and load this data into an NHS England Azure Data Factory and PowerBI reporting solution.

3 PROCESSING OF PERSONAL DATA

- 3.1 The parties have agreed that from the Commencement Date, the terms of this Agreement will apply to and govern all Processing of Personal Data by the Supplier pursuant to the Supply Agreement.
- 3.2 The Parties acknowledge that for the purposes of the Data Protection Legislation and the delivery of the Data Processing Services:
 - 3.2.1 For Personal Data processed in relation to sections 2.1.1 and 2.1.2, NHS England is a Processor, acting on behalf of the employing organisations (local employers) who collect and hold staff personal data in, which is shared to the DSP. The Supplier represents a Sub-processor.
 - 3.2.2 The Supplier acting as a Sub-processor to NHS England will notify NHS England that Condatis will be the operator of the Credential Gateway component and that it has entered into a written agreement with Condatis that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the NHS England's written request, will provide copies of the relevant excerpts from such contract.
 - 3.2.3 For section 2.2, NHSE is the Data Controller and the Supplier is the Data Processor
- 3.3 The Supplier shall notify NHS England immediately if it considers that any of NHS England's instructions infringe the Data Protection Legislation.

- 3.4 The Supplier shall provide all reasonable assistance to NHS England in the preparation of any relevant Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of NHS England, include:
 - 3.4.1 a systematic description of the envisaged Processing operations and the purpose of the processing;
 - 3.4.2 an assessment of the necessity and proportionality of the Processing operations in relation to the Data Processing Services;
 - 3.4.3 an assessment of the risks to the rights and freedoms of natural persons; and
 - 3.4.4 the Protective Measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
- 3.5 The Supplier shall provide all reasonable assistance to NHS England if the outcome of the Data Protection Impact Assessment leads NHS England to consult the Information Commissioner.
- 3.6 The Supplier shall, in relation to any Personal Data processed in connection with its obligations under this Agreement :
 - 3.6.1 process that Personal Data only in accordance with the instructions set out in Appendix 1, unless the Supplier is required to do otherwise by Law. If it is so required, the Supplier shall promptly notify NHS England before processing the Personal Data unless prohibited by Law.
 - 3.6.2 ensure that it has in place Protective Measures to protect against a Data Loss Event having taken account of the:
 - 3.6.2.1 nature of the data to be protected;
 - 3.6.2.2 harm that might result from a Data Loss Event;
 - 3.6.2.3 state of technological development; and
 - 3.6.2.4 cost of implementing any measures.
 - 3.6.3 ensure that:
 - 3.6.3.1 the Supplier Personnel do not process the Personal Data except in accordance with this Agreement (and in particular Appendix 1)

- 3.6.3.2 it takes all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that they:
 - 3.6.3.2.1 are aware of and comply with the Supplier's duties under this clause;
 - 3.6.3.2.2 are subject to appropriate confidentiality undertakings with the Supplier or any Supplier Sub-processor that are in writing and are legally enforceable;
 - 3.6.3.2.3 are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in advance and in writing to do so by NHS England or as otherwise permitted by this Agreement.
 - 3.6.3.2.4 have undergone adequate training in the use, care, protection and handling of Personal Data that enables them and the Supplier to comply with their responsibilities under the Data Protection legislation and this agreement. The Supplier shall provide NHS England with evidence of completion and maintenance of that training within three Working Days of request by NHS England.
- 3.6.4 Not transfer Personal Data outside of the EU unless the prior written consent of NHS England has been obtained and the following conditions are fulfilled:
 - 3.6.4.1 NHS England or the Supplier has provided appropriate safeguards in relation to the transfer as determined by NHS England;
 - 3.6.4.2 the Data Subject has enforceable rights and effective legal remedies;
 - 3.6.4.3 the Supplier 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 NHS England in meeting its obligations) and;

- 3.6.4.4 the Supplier complies with any reasonable instructions notified to it in advance by NHS England with respect to the Processing of the Personal Data.
 - 3.6.5 at the written direction of NHS England, delete or return the Personal Data (and any copies of it) to NHS England on termination of this agreement unless the Supplier is required by Law to retain the Personal Data. If the Supplier is asked to delete the Personal Data the Supplier shall provide NHS England with evidence that the Personal Data has been securely deleted in accordance with the Data Protection legislation within a reasonable period agreed within the written direction of NHS England.
- 3.7 Taking into account the state of the art, the cost 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, the Supplier shall implement Protected Measures to ensure a level of security appropriate to the risk, including, but not limited to, as appropriate:
 - 3.7.1 the pseudonymisation and encryption of Personal Data;
 - 3.7.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - 3.7.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
 - 3.7.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.
 - 3.7.5 to support and investigate any issues encountered post Private Beta Go-Live of the Digital Staff Passport system during ad hoc 3rd line service and deployment support.
- 3.8 Before allowing any Supplier Sub-processor to process any Personal Data related to this agreement, the Supplier must:
 - 3.8.1 notify NHS England in writing of the intended Supplier Sub-processor and Processing, save where such intended Supplier Sub-processor has been specified in the Supplier's response to the Supply Agreement.
 - 3.8.2 obtain the written consent of NHS England save where such intended Supplier Sub-processor has been specified in the Supplier's response to the Supply Agreement.

- 3.8.3 enter into a written agreement with the Supplier Sub-processor which gives effect to the terms set out in this agreement such that they apply to the Processor and in respect of which NHS England is given the benefits of third-party rights to enforce the same; and
 - 3.8.4 provide NHS England with such information regarding the Supplier Sub-processor as NHS England may reasonably require.
- 3.9 The Supplier shall ensure that the third party's access to the Personal Data terminates automatically on termination of this agreement for any reason save that the Supplier and Supplier Sub-processor may access the Personal Data in order to securely destroy it.
- 3.10 The Supplier shall remain fully liable for all acts or omissions of any Supplier Sub-processor.
- 3.11 Subject to clause 3.14, the Supplier shall notify NHS England immediately if it:
 - 3.11.1 receives a Data Subject Access Request (or purported Data Subject Access Request) connected with Personal Data processed under this agreement;
 - 3.11.2 receives a request to rectify, block or erase any Personal Data connected with Personal Data processed under this agreement;
 - 3.11.3 receives any other request, complaint or communication relating to either party's obligations under the Data Protection Legislation connected with Personal Data processed under this agreement;
 - 3.11.4 receives any communication from the Information Commissioner or any other Supervisory or Regulatory Body connected with Personal Data processed under this agreement;
 - 3.11.5 receives a request from any third party for disclosure of Personal Data connected with this agreement; or
 - 3.11.6 becomes aware of an actual or suspected Data Loss Event.
- 3.12 This notification shall be given by emailing the original request and any subsequent communications to england.ig-corporate@nhs.net.
- 3.13 The Supplier shall not respond substantively to the communications listed at clause 3.11 save that it may respond to a Regulatory or Supervisory Body following prior consultation with NHS England.

- 3.14 The Supplier's obligation to notify under clause 3.11 shall include the prompt provision of further information to NHS England in phases, as details become available.
- 3.15 Taking into account the nature of the Processing, the Supplier shall provide NHS England with full assistance in relation to either party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 3.11 (and insofar as possible within the timescales reasonably required by NHS England) including by promptly providing:
- 3.15.1 NHS England with full details and copies of the complaint, communication or request;
 - 3.15.2 such assistance as is reasonably requested by NHS England to enable NHS England to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
 - 3.15.3 such reasonable assistance as is reasonably requested by NHS England to enable NHS England to comply with other rights granted to individuals by the Data Protection Legislation including the right of rectification, the right to erasure, the right to object to processing, the right to restrict processing, the right to data portability and the right not to be subject to an automated individual decision (including profiling);
 - 3.15.4 NHS England at its request, with any Personal Data it holds in relation to a Data Subject;
 - 3.15.5 such reasonable assistance as requested by NHS England following any Data Loss Event;
 - 3.15.6 such reasonable assistance as requested by NHS England in relation to informing a Data Subject about any Data Loss Event, including communication with the Data Subject;
 - 3.15.7 such reasonable assistance as requested by NHS England with respect to any request from the Information Commissioner's Office, or any consultation by NHS England with the Information Commissioner's Office;
 - 3.15.8 NHS England with any copies of requests from Data Subjects seeking to exercise their rights under the Data Protection Legislation under this agreement. Such requests must be sent to england.dpo@nhs.net immediately, and in no longer than one Working Day of receipt by the Supplier.

- 3.16 The Supplier shall allow for reasonable audits of its delivery of the Data Processing Services by NHS England or its designated auditor.
- 3.17 The Supplier shall provide NHS England with evidence to demonstrate compliance with all of its obligations under this agreement and the relevant Data Protection Legislation.
- 3.18 The Supplier shall designate a Data Protection Officer (DPO) if required by the Data Protection legislation and shall communicate to NHS England the name and contact details of any DPO.
- 3.19 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this agreement, the Data Protection legislation and Data Guidance. The Supplier must create and maintain a record of all categories of data processing activities carried out under this agreement, containing:
 - 3.19.1 the categories of Processing carried out under this agreement;
 - 3.19.2 where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, where relevant, the documentation of suitable safeguards;
 - 3.19.3 a general description of the Protective Measures taken to ensure the security and integrity of the Personal Data processed under this agreement; and
 - 3.19.4 a log recording the Processing of Personal Data in connection with this agreement comprising, as a minimum, details of the Personal Data concerned, how the Personal Data was processed, where the Personal Data was processed and the identity of any individual carrying out the Processing.
- 3.20 The Supplier shall ensure that the record of processing maintained in accordance with clause 3.19 is provided to NHS England within five Working Days of a written request from NHS England.
- 3.21 This agreement does not relieve the Supplier from any obligations conferred upon it by the Data Protection Legislation.
- 3.22 The parties agree to take account of any guidance issued by the Information Commissioner. NHS England may on not less than thirty Working Days' notice to the Supplier amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner.

- 3.23 NHS England may, at any time on not less than thirty Working Days' notice, revise this clause by adding to it 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).
- 3.24 The Supplier warrants and undertakes that it will deliver the Data Processing Services in accordance with all Data Protection legislation, any Data Guidance and this Agreement and in particular that it has in place Protective Measures that are sufficient to ensure that the delivery of the Data Processing Services complies with the Data Protection Legislation and ensures that the rights of Data Subjects are protected. Neither party shall do or omit to do anything that will put the other party in breach of the Data Protection Legislation or the Data Guidance.
- 3.25 The Supplier shall, at all times during and after the expiry of this Agreement, indemnify NHS England and keep NHS England indemnified against all losses, damages, costs or expenses and other liabilities (including legal fees) incurred by, awarded against or agreed to be paid by NHS England arising from any breach of the Supplier's obligations under this clause with a Liability cap of £5million.
- 3.26 The Supplier must reasonably assist NHS England in ensuring compliance with the obligations set out at Article 32 to 36 of the UK GDPR and equivalent provisions implemented into Law, taking into account the nature of processing and the information available to the Supplier.
- 3.27 Each party must take prompt and proper remedial action regarding any Data Loss Event.
- 3.28 The Supplier must reasonably assist NHS England by taking appropriate Protective Measures, insofar as this is possible, for the fulfilment of NHS England's obligation to respond to requests for exercising rights granted to individuals by the Data Protection Legislation.

4 INTERNATIONAL PERSONAL DATA TRANSFERS

- 4.1 The Supplier (and any Supplier Sub-processor) must not transfer or otherwise process the Personal Data outside the UK without first obtaining the written consent of NHS England.
- 4.2 Where such consent is granted, the Supplier may only process, or permit the processing, of the Personal Data outside the UK under the following conditions:
 - 4.2.1 the Supplier is Processing the Personal Data in a territory which is subject to adequacy regulations under the Data Protection Legislation

that the territory provides adequate protection for the privacy rights of individuals; or

4.2.2 the Supplier participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that the Supplier (and, where appropriate, NHS England) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the UK GDPR; or

4.2.3 the transfer otherwise complies with the Data Protection Legislation.

4.3 If any Personal Data transfer between NHS England and the Supplier requires execution of an International Data Transfer Agreement (IDTA), or other agreements as approved, the parties will complete all relevant details in, and execute, the IDTA and take all other actions required to legitimise the transfer.

5 TERM AND TERMINATION

5.1 This Agreement shall commence on the Commencement Date. Unless terminated in accordance with this clause, this Agreement shall automatically terminate on termination or expiry of the Supply Agreement.

5.2 Without affecting any other right or remedy available to it, NHS England may immediately terminate this agreement by notice in writing to the Supplier if the Supplier commits a material breach of any provision of this agreement or the Supplier repeatedly breaches any of the provisions of this agreement.

5.3 If NHS England terminates this agreement pursuant to the foregoing clause this shall be deemed an irremediable material breach of the Supply Agreement and NHS England shall be entitled (without affecting any other right or remedy available to it) to immediately terminate the Supply Agreement for the Supplier's irremediable breach of the Supply Agreement without incurring any liability to the Supplier.

5.4 On termination of this agreement:

5.4.1 any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of this agreement which existed at or before the date of termination, shall not be affected;

5.4.2 the provisions of this Agreement which place obligations on the Supplier in respect of the processing of Personal Data shall continue in force and effect until such time as all Personal Data (including all copies thereof) has either been returned and/or destroyed in accordance with the foregoing sub-clause (unless otherwise strictly required by Law);

- 5.4.3 without prejudice to the foregoing sub-clause, the provisions of this Agreement that expressly or by implication are intended to come into or continue in force on or after termination of this agreement shall remain in full force and effect;

6 REMEDIES AND NO WAIVER

- 6.1 The Supplier shall indemnify, defend and hold harmless NHS England from and against all and any losses, claims, liabilities, costs, charges, expenses, awards and damages of any kind including any fines and legal and other professional fees and expenses (irrespective of whether they were reasonably foreseeable or avoidable) which it/they may suffer or incur as a result of, or arising out of or in connection with, any breach by the Supplier of any of its obligations in this Agreement with a liability cap of £5million. For the avoidance of any doubt, any limitation of liability which applies under the Supply Agreement shall not apply to the Supplier's liability under the indemnity in this clause (which shall be limited to £5million).
- 6.2 The rights and remedies provided under this agreement are in addition to, and not exclusive of, any rights or remedies provided by Law or in equity.
- 6.3 A waiver of any right or remedy under this agreement or by Law or in equity is only effective if given in writing and signed on behalf of the party giving it and any such waiver so given shall not be deemed a waiver of any similar or subsequent breach or default.
- 6.4 A failure or delay by a party in exercising any right or remedy provided under this agreement or by Law or in equity shall not constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict any further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy provided under this agreement or by Law or in equity shall prevent or restrict the further exercise of that or any other right or remedy.

7 NOTICES

- 7.1 Any notice given to a party under or in connection with this Agreement shall be in writing in the English language and shall be sent by email to the relevant address set out below.
- NHS England contact email: england.digitalstaffpassport@nhs.net
 - Sitekit contact email: jill.debene@sitekit.co.uk
- 7.2 Any notice validly given in accordance with the foregoing clause shall be deemed to have been received the following Working Day.

8 GENERAL

- 8.1 The Supplier shall not assign, transfer, mortgage, charge, subcontract, declare a trust over or deal in any other manner with any or all of its rights and obligations under this agreement without the prior written consent of NHS England.
- 8.2 No variation of this agreement shall be effective unless it is in writing and signed by the parties to this agreement.
- 8.3 This agreement may be executed in any number of counterparts, each of which when executed and delivered shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement. No counterpart shall be effective until each party has executed at least one counterpart.

9 GOVERNING LAW AND JURISDICTION

- 9.1 This agreement 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) shall be governed by and construed in accordance with the Law of England and Wales.
- 9.2 Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this agreement or its subject matter or formation (including non-contractual disputes or claims), provided that nothing in this clause shall prevent a party from enforcing any judgement obtained in the court of England and Wales in any other court with jurisdiction over the other party.

THIS AGREEMENT has been entered into on the date stated at the beginning of it.

10 REVIEWERS

This agreement must be reviewed by the local Information Asset Owner and one of NHS England's Corporate IG Managers. Please submit this form to england.dpo@nhs.net or to your local IG team.

Reviewed by NHS England's
[INFORMATION ASSET OWNER] as the
Information Asset Owner responsible for the
personal data:



Name of Information Asset Owner

Date

Reviewed by NHS England's [CORPORATE
IG MANAGER] on behalf of Corporate
Information Governance:



Name of Corporate IG Manager

Date

11 SIGNATORIES

To become legally binding, this agreement must be signed by relevant directors from both NHS England and the Supplier.

Signed by [NAME OF DIRECTOR] for and on behalf of NHS England:

[Redacted Signature]

Signature of Director

Name of Director

21st November 2023

Date

Signed by [NAME OF DIRECTOR] for and on behalf of Sitekit Applications Ltd

[Redacted Signature]

Signature of Director

Name of Director

16 November 2023

Date

12 APPENDIX 1 – DATA PROCESSING SERVICES

1. The Supplier shall comply with any further reasonable and relevant written instructions with respect to Processing by NHS England.
2. Any such further instructions shall be incorporated into this Appendix 1.

Description	Details
Subject matter of the processing	<p><i>The Supplier is required to support the testing of the DSP system(s) using data from the Live Electronic Staff Records (ESR) system during the design and build of the system.</i></p> <p><i>The Supplier is to provide third line support to support and investigate any issues encountered post Go-live of the DSP system.</i></p> <p><i>Condatix to support credential gateway user ID/access credential to be provided to verify identity to Portal Administrators.</i></p> <p><i>SiteKit DSP Audit database, where different actions for the different credentials and events, completed by different user types e.g., PGD, temporary staff, HR or other authorised users.</i></p>
Duration of the processing	<i>Private beta stage.</i>
Nature and purpose of the processing	<p><i>The DSP Employer's and Employee's portal holds staff members' essential information - including personal, employment (excluding pay), skills and occupational health. So, when they want to move between NHS organisations, they can quickly and securely transfer the information that's required, without duplicate form filling, checks and training. The focus being on Postgraduate doctors when they rotate and staff moving on a temporary basis to work at a different NHS organisation.</i></p> <p><i>As well as storing self-declared data provided by the staff member, data is also retrieved and stored from the ESR (Electronic Staff Record) system before credentials are issued back to the staff member in a secure wallet (out of scope for Supplier Processing)</i></p> <p><i>All DSP data is stored in the secure NHS Azure tenant as described previously, which is held in the UK.</i></p> <p><i>Audit data for NHSE managed PowerBI reporting containing event logs of actions and outcomes from different user types (e.g., Portal Administrators, PGDs, system).</i></p>

	<p><i>The reporting solution aims to provide Organisations with a detailed and factual understanding of the nature of their staff movements, the types of onboarding and hiring activity experienced, and how Portal Administrators have managed that activity. Organisations can then use this improved understanding to consider how they can better respond to their ongoing staff movements, improve quality and management of the hiring and onboarding processes, and explore how more efficient use of resources may improve the experience (for the clinical staff moving, and their workforce managing the administration for it). Furthermore, it will enable organisations to see the benefit from adopting the DSP and what efficiencies and improvements they have achieved through implementing it.</i></p> <p><i>The reporting solution for NHS England use will be used to demonstrate how the NHS Digital Staff Passport can support efficient movement of staff across NHS organisations, to save time for movers and Portal Administrators by easing the administrative burden, eliminating duplication and enabling consistent onboarding and access to organisational information.</i></p> <p><i>This reporting solution will enable the programme board to demonstrate benefits aligned to the three key strategic objectives for the DSP, as a key constituent to support the business case. Furthermore, it will include reports on the mandatory GDS/CDDO KPIs for reporting on the performance of the DSP service, along with other important housekeeping metrics related to uptake and usage.</i></p>
Type of Personal Data	<ul style="list-style-type: none"> • <i>Name, address, nationality, date of birth</i> • <i>Identity Photograph</i> • <i>Basic details relating to employment checks – including DBS and right to work information;</i> • <i>Professional registration details (GMC/NMC/GDC/HPC) where applicable;</i> • <i>Basic details relating to current employment – including employing organisation, job role, staff group, start date, pay band, work email address, smartcard number, area of work, job title, and,</i> • <i>Occupational Health clearance confirmation including Immunisation and Vaccinations, OH contact number, email address</i> <p><i>The following data items will be captured if a staff member uses the digital staff passport to perform a temporary move:</i></p> <ul style="list-style-type: none"> • <i>Temporary placement start date & end date</i>

	<ul style="list-style-type: none"> • <i>Details of temporary role such as department, position title, position number, description of work pattern and department contact details</i> • <i>HR contact</i> • <i>Approved by</i> <p><i>The following data items are optional for the staff member to provide within the person credential;</i></p> <ul style="list-style-type: none"> • <i>Maiden name,</i> • <i>National Insurance number</i> • <i>Preferred Pronouns</i> • <i>Gender</i> • <i>Passport number</i> • <i>Driving License number</i> • <i>Phone number</i> • <i>Ethnic category</i> • <i>Country of birth</i> • <i>Religious beliefs</i> • <i>Sexual orientation</i> • <i>Next of kin details</i> • <i>2 Emergency contact details</i> • <i>Marital status</i>
Categories of Data Subject	<i>Postgraduate doctors & NHS staff moving on a temporary basis</i>

13 APPENDIX 2 - BACKGROUND

NHS England has appointed the Supplier to provide the Services (as defined below) under an agreement dated 26/07/23 (the Supply Agreement) for the provision of the design and build of the Digital Staff Passport solution. NHS England (Corporate IT & Smarter Working) will manage the live deployments and provide an ongoing managed service, while the Supplier will provide ad hoc deployment and 3rd line support where required. This Data Processing Agreement is limited to the Private Beta Stage.

NHS England has agreed to provide such Personal Data to the Supplier for Processing only in accordance with the terms of this Agreement from the date on which this Agreement is entered into (the Commencement Date).

The Digital Staff Passport contains different solution components and interoperates with other services. The table below defines each of the components and external services.

Primary solution:

- The primary solution component is the Digital Staff Passport

Sub-components include:

- Employer's portal for use by local Employer's portals
- Employee's portal for use by staff members
- Credential Gateway to manage the exchange of credentials with Digital Wallets (an app that uses authentication and data encryption software to protect credentials downloaded into it).
 - The Credential Gateway is delivered by the Supplier via a sub-contract with Condatis Group Ltd, and the Credential Gateway handles the interfaces to Digital Wallets and Identity Providers (providers are certified as meeting relevant industry security standards and the Identity Assurance Principles published by the Cabinet Office and the National Cyber Security Centre (NCSC)).
- Audit database to record transactions where the transaction data is used by external tools operated by NHS England to create management reports.

External services include:

- Interface to NHS Mail to exchange emails
- Interface to Azure AD to enable login by local authorised users, e.g. HR, medical staffing, training, education and occupational health teams
- Interface to Gov.Notify to send notifications to staff members
- Interface to ESR to access details about an employee for the organisation where the employee is employed
- Interface to approved Identity Providers for identity verification of staff, e.g. Yoti

To the extent that the Supply Agreement contains any provisions which govern the Processing of Personal Data by the Supplier, the parties agree and acknowledge that the provisions of this Agreement shall prevail to the extent of such conflict or inconsistency.

Schedule 9: NHS Digital Staff Passport Technical Supplier: Clarifications Response Document



NHS Digital Staff Passport Technical Supplier

Clarifications Response Document

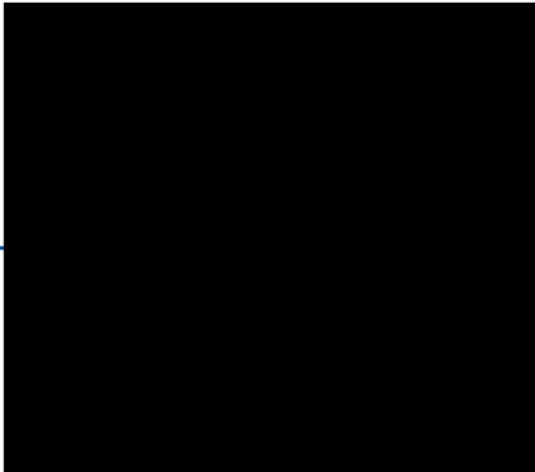
Lesley Erskine
Sitekit

CONFIDENTIAL

Classification: Official

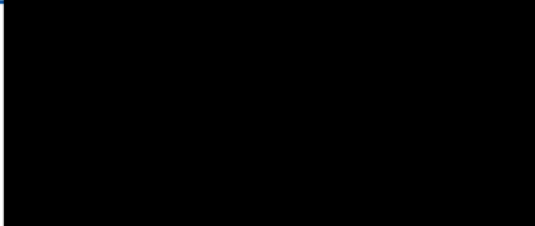
Document Control:

Title:
Owner:
Classification:




Version Information:

Last Reviewed:
Reviewed By:
Last Published:
Published By:
Published Version:



@
This document is uncontrolled when printed or sent as an attachment

Change Log:

Version	Date	By	Changes
0.1	24/11/2023		

Classification: Official

Contents

1. Aim: 4

2. Background: 4

3. Requirements: 5

 3.1 Functions required for NHS organisation portals and credential gateway. 5

 3.2 Functional deliverables required 5

 3.3 Process required: 7

4. Target Outcomes: 11

5. Payment: 11

6. Key Performance Indicators: 12

8. Procurement Timetable (Indicative) 13

9. Evaluation Process 13

10. Scoring Criteria 14

11. Clarification Questions for Supplier Response..... 15

Classification: Official

Request for Clarifications

NHS Digital Staff Passport_ Technical Supplier

via G-Cloud 13

1. Aim:

- 1.1 The NHS Digital Staff Passport (DSP) is currently in private beta development. NHS England are looking to award an interim contract for a technical supplier to run from 11th December 2023 to 30 August 2024. The interim contract will ensure the DSP is stable enough to roll out the private beta and gather detailed requirements for the public beta.
- 1.2 The purpose of this document is to provide a brief to shortlisted suppliers of our requirements to enable them to determine whether they can meet our specifications, match our services and that they have the capacity and availability for call-off and to clarify how they will deliver the specified requirements within the allocated time.

2. Background:

- 2.1 The NHS has committed in the [Long Term Plan](#) to enable "staff to move more easily from one NHS Employer to the other". This was emphasised in the Interim People Plan and re-emphasised in subsequent versions. The [2023/24 NHS operational planning guidance](#) also speaks to the need for flexible workforce deployment of staff across organisational boundaries using digital solutions such as the Digital Staff Passport. The long awaited [Long Term Workforce Plan](#) now expects the full roll out of the Digital Staff Passport by August 2025. This procurement is therefore critical to the delivery of a key NHS ambition to enable staff to move.
- 2.2 **The NHS Digital Staff Passport (DSP)** is a trusted and secure digital means by which NHS employees can digitally transfer their key employment data between different NHS employers and into their respective workforce systems. The DSP facilitates an adaptable and agile workforce who can move seamlessly between NHS Trusts in a way that safeguard services and patients.
- 2.3 To enable rapid deployment of key workers in support of the NHS response to COVID-19, the DSP development was accelerated. This led to the interim COVID-19 DSP, a solution that enabled securely sharing a point-in-time snapshot of a staff member's employment status, so that the worker does not need to repeat employment checks when they were temporarily deployed in response to the COVID-19 pandemic. The evolution of this interim COVID-19 DSP is the new NHS DSP, which will enable secure transfer of key staff employment check information.

Classification: Official

3. Requirements:

3.1 Functions required for NHS organisation portals and credential gateway.

- Project management
- Proxy product ownership (UCD and Technical)
- UCD
- Technical application development, including API development.
- Development Operations (DevOps)
- Quality assurance
- Testing
- 2nd and 3rd line support

3.2 Functional deliverables required.

- New and enhanced requirements after Minimum Viable Product (MVP) release for the DSP service covering both the NHS organisations' portals and the credential gateway.
- Project management / Product Owners
 - Collaborative working with the Authority's Project managers / Delivery Lead to co-ordinate different suppliers, meetings, follow-up meeting notes etc.
 - Weekly Programme Board reporting
 - Sprint ceremonies – sprint planning, sprint demonstrations, sprint retrospectives
 - Leading elaboration sessions on business requirements
- Backlog / sprint management
 - Requirements/Stories and Acceptance Criteria captured in DevOps – refined through initial requirements from the Authority's product lead, elaboration sessions, approved UCD and detailed acceptance criteria for developers/testers before the commencement of development work.
 - Estimates for Requirements/Stories (in Story Points) within DevOps
 - Running sprint planning, demo and retros for UCD and development teams that includes the Authority's product lead / technical product owner to ensure stories are fully understood, prioritisations are clear.
 - ❖ *The Authority's Product Lead and Technical Product Owner will make all prioritisation decisions for the sprint and will require their approval to move stories from one sprint to the next.*
 - Daily stand ups.
- Solution architecture.
 - Elaboration, validation and sign off requirements within joint elaboration sessions. Attended as a minimum by the supplier product owner, lead architect and developer.

Classification: Official

- ❖ the Authority's Product lead and technical product owner to be involved in these elaboration sessions with the supplier development team to ensure requirements are fully understood before planning and development starts.
- Update of technical documentation, where relevant.
- UCD.
 - Elaboration, validation and sign off requirements within joint elaboration sessions. Attended as a minimum by supplier product owner, lead architect and developer.
 - Live design sessions for features that require collective sign off.
 - Design documentation kept up to date with relevant details for testing team.
 - UCD following NHS Service Manual, W3C accessibility standards, content consistency.
- Development.
 - Elaboration, validation and sign off requirements within joint elaboration sessions. Attended as a minimum by the supplier product owner, lead architect and developer.
 - ❖ the Authority's product lead and technical product owner to be involved in these elaboration sessions with the supplier development team to ensure requirements are fully understood before planning and development starts.
 - Update of technical documentation, where relevant.
- QA / Testing.
 - Sprint planning to ensure acceptance criteria is clearly defined ahead of start of development.
 - Test scripts.
 - Release notes.
 - Regression testing
 - ❖ Ensuring no new defects are introduced with defect fixes and new features.
 - Defect management process.
- DevOps.
 - Optimisation of deployment process.
 - Maintenance of deployment process documentation / installation guide.
- 2nd and 3rd line support
 - Service commitments as outlined in table below.
 - Options for dedicated support team to incidents triaging and fixing can be prioritised into a sprint, with acknowledgement that P1 and P2 issues may disrupt the ongoing sprint and P3-P5 issues will need to be triaged before being planned in.
 - Completion and communication of Service Request, Incident or Problem Resolution

Classification: Official

Operational hours (service hours)	24x7x365
Business support hours (service support hours)	8 – 6pm Monday to Friday (excluding Bank Holidays)
Availability (in business support hours)	99.5% (with an aim to move to 99.9.%)
Incident resolution times (in business support hours)	
Severity 1	4 hours
Severity 2	8 hours
Severity 3	20 hours
Severity 4	80 hours
Problem fix times	
Severity 1	30 working days or an agreed release
Severity 2	60 working days or an agreed release
Severity 3	120 working days or an agreed release
Severity 4	240 working days or an agreed release
Service reporting	Monthly
Disaster recovery	4 hours
Recovery point objective (RPO)	24 hours

3.3 Process required:

3.3.1 The Authority requires sprints of 2-weeks duration (10 working days) of the following size (in story points) for:

- UCD: 15- 25 story points per sprint.
- Application development: 75 – 85 story points per sprint
- Supplier to work closely with the Authority's product lead / technical product owner to review assigned story points within sprint planning sessions.
- Supplier to apply Fibonacci sequencing to ascertain story points (1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144)
- DSP product backlog requirements which extend beyond the 75 to 85 story points for a sprint will be organised as Epics, Features and then Stories to breakdown the story points for the requirement. This means stories can be completed within one sprint, whilst the overall epic / feature will then be delivered across multiple sprints.
- 2nd and 3rd line support queries to be prioritised into the sprint as their occur. P1, P2 issues may disrupt an ongoing sprint, P3-P5 issues to be planned in.

Classification: Official

- 3.3.2. The Authority will manage the releases for Production deployments with support from the supplier. The supplier's requirement is for:
- All features and functionality to be tested and signed off within UAT environment and preparing deployment packages for other environments (training, pre-production, production).
 - The supplier to ensure a branching strategy is adhered to ensure product backlog functionality development is managed within lower environments and can be deployed into UAT environments for testing.
 - The supplier to work closely with the Authority's release manager to ensure only approved product backlog features are deployed into the relevant environment.
- 3.3.3. The Authority requires best practice governance of sprint / release approval process. The following sprint approval checklist agreed at a minimum agreed and in place before each discrete sprint starts:
- **Sprint goal:** this is the overarching objective that the team is trying to achieve for the sprint.
 - **Backlog items:** these are the specific tasks that need to be completed in order to achieve the sprint goal.
 - **Definition of Done:** this is a list of criteria that must be met for a backlog item to be considered complete.
 - **Acceptance criteria:** these are the specific requirements that must be met for a backlog item to be accepted by the product owner.
 - **Sprint tasks:** these are the smaller tasks that need to be completed in order to complete a backlog item.
 - **Sprint burndown chart:** this chart tracks the team's progress towards completing the sprint backlog.
 - **Sprint review:** this meeting is held at the end of the sprint to demonstrate the work that has been completed.
 - **Sprint retrospective:** this meeting is held at the end of the sprint to discuss what went well, what could be improved, and how the team can work more effectively in the next sprint.
 - Visibility of the supplier's internal retrospectives to feed into monthly sprint retrospective with the Authority.
 - **Impediments:** these are any roadblocks or challenges that are preventing the team from completing the sprint backlog.
 - **Documentation:** this includes any documentation that was created during the sprint, such as user stories, wireframes, or code comments.
 - **Testing:** this ensures that the work that was completed in the sprint meets the quality standards.

Classification: Official

- **Deployment:** this is the process of making the work that was completed in the sprint available to users.

3.3.4. The Authority requires the following to be documented and agreed to have taken place before a release is approved.

- **Project name, team and client:** this information helps to identify the release and the people involved.
- **Release number and date:** this information helps to track the release and ensure that it is properly scheduled.
- **Release goals and objectives:** this information helps to ensure that the release is aligned with the project's overall goals.
- **Requirements:** this information ensures that the release meets the needs of the users.
- **Dependencies:** this information identifies any other releases or systems that the release depends on.
- **Testing:** this information ensures that the release is tested and ready for deployment.
- **Deployment plan:** this information describes how the release will be deployed to production.
- **Rollback plan:** this information describes how to roll back the release if necessary.
- **Communication plan:** this information describes how the release will be communicated to the users.
- **Documentation:** this information provides documentation for the release, such as user guides and release notes.
- **Approvals:** This information ensures that the release has been approved by all stakeholders.
- **Post-release activities:** This information describes the activities that will be performed after the release, such as monitoring and maintenance.

3.3.5. The Authority requires best practice format for sprint demonstration and retrospective. Agenda as follows.

- **Sprint demonstration agenda**
 - **Completed work:** the team should demonstrate the work that they have completed during the sprint. This could include new features, bug fixes, or improvements to existing functionality.
 - **Acceptance criteria:** the team should demonstrate that the work meets the acceptance criteria that was agreed upon with the product owner.
 - **User stories:** the team should explain the user stories that were implemented during the sprint. This helps to ensure that the work is aligned with the needs of the users.

Classification: Official

- **Questions and feedback:** the team should be open to questions and feedback from the product owner, stakeholders, and other team members. This helps to ensure that the work meets the expectations of everyone involved.
- **Next steps:** the team should discuss the next steps for the product. This could include planning the next sprint, releasing the work to production, or gathering more feedback from users.
- **Sprint retrospective agenda**
 - **What went well?** this is an opportunity for the team to celebrate its successes and learn from them.
 - **What could be improved?** this is where the team can identify areas for improvement and make plans to address them.
 - **What will we commit to improving in the next sprint?** this is where the team makes specific commitments to improve their processes and results.
 - **Review of Story Point Estimates:** report on accuracy of estimates +/- and actions to improve. Identification of areas of trends.
 - **Action items:** the team should come up with specific actions that they will take to address the areas for improvement. These actions should be assigned to specific people and have due dates.
 - **Follow-up:** the team should schedule a follow-up meeting to discuss the progress of the action items.
 - **Continual Service Improvement (CSI) Sprint Retrospective Questions:**
 - ❖ What were the biggest challenges we faced?
 - ❖ How can we communicate better with each other?
 - ❖ How can we make our work environment more efficient?
 - ❖ How can we improve our testing process?
 - ❖ How can we get better feedback from users?
 - ❖ What are our goals for the next sprint?
 - ❖ What are the risks and challenges we need to be aware of?

Classification: Official

4. Target Outcomes:

High level roadmap for post MVP release is outlined below which is planned to be one release per month – to be confirmed with the Authority. The target outcome for this contract is as follows:

- Release 8 / 9 – January 2024
- Release 9 / 10 – February 2024
- Release 10/ 11 – March 2024 (scope to be confirmed based on private beta feedback)
- Release 12 – April 2024 (scope to be confirmed based on private beta feedback)
- Release 13 – May 2024 (scope to be confirmed based on private beta feedback)
- Release 14 – June 2024 (scope to be confirmed based on private beta feedback)
- Release 15 – July 2024 (scope to be confirmed based on private beta feedback)
- Release 16 – August 2024 (scope to be confirmed based on private beta feedback)

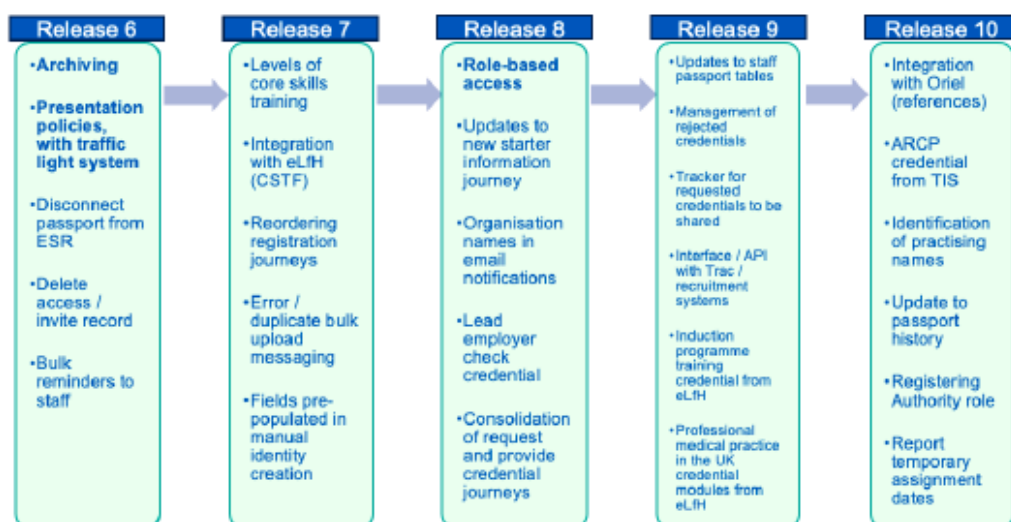


Figure 1: High level release plan

Reprioritisation of features in each release on approval of the Authority's product lead / technical product owner only.

5. Payment:

The payment profile for this contract is monthly in arrears; payment will be made on successful delivery of sprints, approved and signed-off as acceptable by the Authority's Product Lead / Technical Product Owner.

Classification: Official

6. Key Performance Indicators:

Key Performance	Metric	Measurement
Project Governance	Timely and accurate highlight reports detailing status, progress against timeline, dependencies, risks, issues and tracking against budget.	<ul style="list-style-type: none"> • Weekly reports
	Maintenance of roadmap and detailed workplan	<ul style="list-style-type: none"> • Weekly / fortnightly updated workplan
	Participation at regular stand ups and update meetings with team leadership	<ul style="list-style-type: none"> • Weekly attendance • Preparedness for meeting • Good input in update/discussions
	Attendance and presenting at regular governance meetings, including preparing papers in advance	<ul style="list-style-type: none"> • Attendance, as required. • Preparedness for meeting • Quality of presentation materials
	Providing materials to aid senior decision-making	<ul style="list-style-type: none"> • Availability for ad hoc requests • Quality of material
Stakeholder management	Attendance and presenting at key stakeholder meetings, including preparing papers in advance.	<ul style="list-style-type: none"> • Weekly / monthly attendance • Preparedness for meeting • Good input in update/discussions • Quality of materials
	Developing and maintaining relationships with key suppliers and stakeholders	<ul style="list-style-type: none"> • Feedback from key suppliers and stakeholders on the good relationship
Collaboration	Collaborative approach with suppliers and stakeholders to ensure co-design and sharing of expertise and knowledge	<ul style="list-style-type: none"> • Evidence of participation in the network, and input and feedback regarding specs
Effectiveness	Response to identified issues.	<ul style="list-style-type: none"> • Time taken to respond to identified issues.

Classification: Official

8. Procurement Timetable (Indicative)

Date (2023)	Activity
Wednesday 15 th November.	Request for clarification shared with shortlisted suppliers.
Monday 20 th November	Deadline for Clarification Questions
Monday 27 th November, 12 noon	Deadline for submission
Tuesday 28 th – Wednesday 29 th November	Evaluation of submissions
Thursday 7 th December	Contract award notification
Monday 11 th December	Contract start / kick of meeting

9. Evaluation Process

9.1 The purpose of evaluation in the procurement process is to establish the supplier's Proposal provides value for money to the Authority.

9.2 The Authority reserves the right to accept or reject all or any part of the Proposal if you have failed to provide the information requested or have submitted any modification or any qualification to the terms and conditions of contract.

9.3 The Authority does not bind itself to accept the quotation, nor guarantee any value or volume and shall not be liable to accept any costs you have incurred in the production of your quotation. The Authority will check the supplier's quotation for completeness and compliance with the requirements in this clarification document, thus, you should ensure that you carefully examine this document in full.

9.4 Proposals will be evaluated on the following Quality and Costs basis.

Section	Weighting (%)
Technical/Quality	100%
Commercial/Fixed Price	As per Framework Rate Card

Please submit your **fixed price** (supported by a comprehensive breakdown of cost) for this work, in-line with the rate card provided at G-Cloud 13.

Classification: Official

10. Scoring Criteria

The supplier submissions will be scored against the quality criteria as follows:

Score	Assessment	Interpretation
5	Very high Standard	Excellent level of detail and assurance - no reservations about acceptability and elements of meaningful added value included.
4	High Standard	Excellent level of detail and assurance - only very minor reservations present and aspects of added value may be present, but these are not considered material.
3	Reasonable Standard	Sufficient level of detail and assurance - some reservations about acceptability. Added value may be present.
2	Limited Standard	Limited level of detail and significant reservations around acceptability.
1	Not Acceptable	Insufficient detail has been provided and/or the response gives major cause for concern.

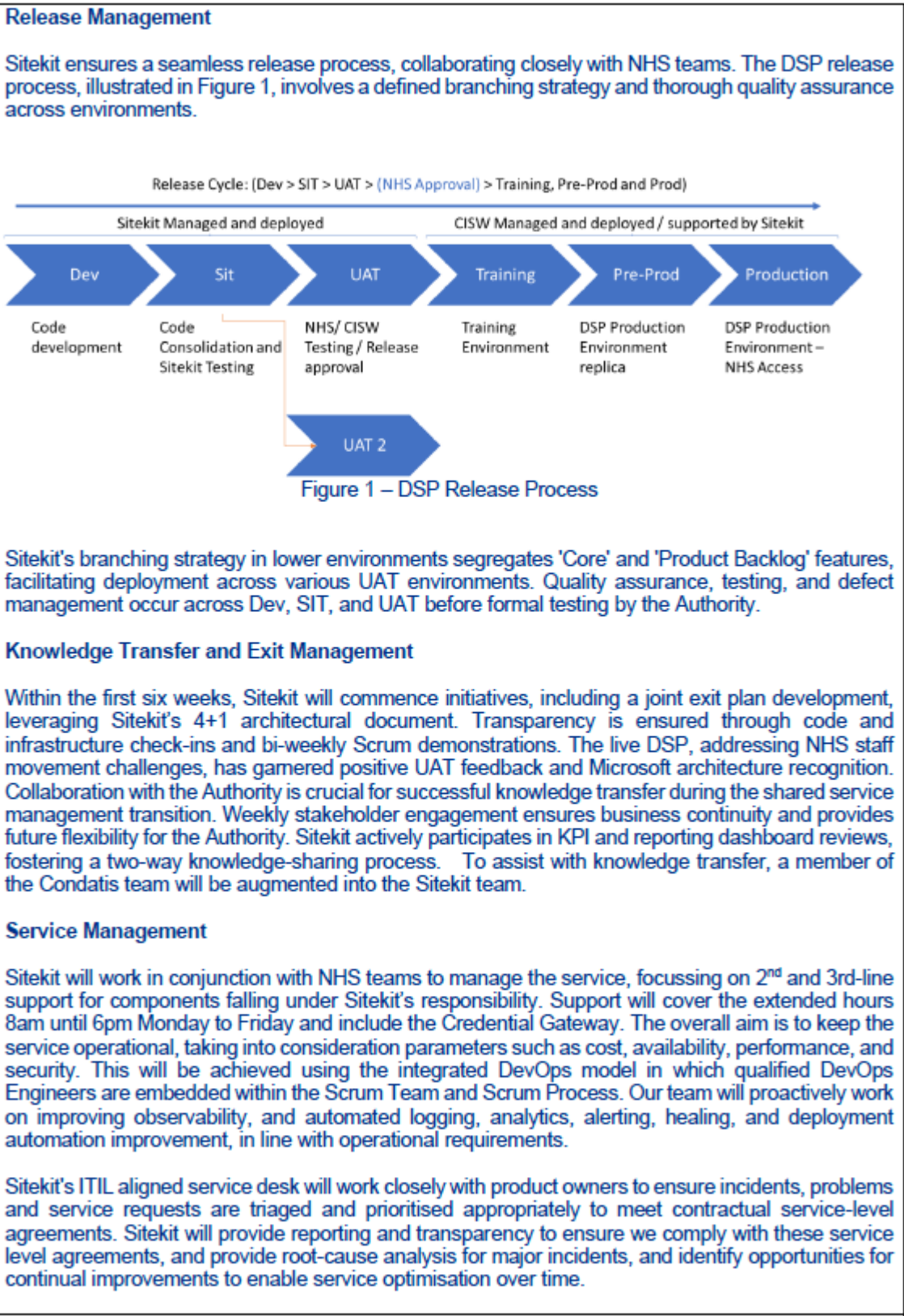
Sitekit would like to thank NHS England for the opportunity to respond to these Clarification Questions. Sitekit acknowledges that the above information has been read and understood. For ease of reference all Sitekit responses are in Blue Font.

Classification: Official

11. Clarification Questions for Supplier Response.

Clarification Question	Max Word Limit	Weighting
Q1 – Approach Overview:		
<p>Please provide an overview describing your approach to delivering the Authority's specified requirements.</p> <p>Your response should cover, but not limited to your approach to knowledge transfer during contract delivery and exit management at the conclusion of the contract.</p>	750 words	40%
<p>Approach Overview</p> <p>Sitekit, a Microsoft Managed Services Partner, excels in Azure and Entra, collaborating with Microsoft on complex identity integrations. Recognised for delivering DID interoperability, the award-winning NHS DSP solution has evolved with Microsoft's support. Our multidisciplinary team follows a robust implementation methodology, integrating Scrum, Secure Development Lifecycle, and DevOps for effective service management. Key to success is our close partnership with Microsoft, influencing product development and utilising certified DevOps Engineers, Administrators and Architect Experts for hosting in Azure. Skilled professionals drive our delivery phases, ensuring excellence in project management, product ownership, architecture, UCD, software development, QA, testing, and support.</p> <p>Azure Dev Ops / Sprint Management</p> <p>Sitekit leverages Azure Dev Ops for effective Sprint Management, following Scrum ceremonies over a 10-day period.</p> <p>Key steps include:</p> <ul style="list-style-type: none"> • Sprint Planning: Story Points are defined and agreed upon by all Product Owner's with task management in Dev Ops. • Sprint Demonstrations: End-to-end DSP demos are provided to stakeholders. • Sprint Retrospectives: Internal retrospectives occur at the end of each Sprint, providing continuous improvement and influencing the next cycle. Monthly retrospectives with NHS Product Owners consolidate feedback. • Sprint Sign Off: All stories are reviewed, and Product Owners from Sitekit and NHS sign off, updating planning documentation accordingly. 		

Classification: Official



Classification: Official

Condatis Credential Gateway (CCG)

This contract delivers the retention of the current staging environment and production environment for use up to 100 trusts and a total transaction capacity of 1,000,000. The production environment will include live PII and the agreed security hardening infrastructure will be deployed and monitored as part of the SLA.

Sitekit have agreed with Condatis to provide an option to simplify production support and data processing requirements for the NHS, the Condatis Credential Gateway Production instance could be hosted and run within an NHS owned Microsoft Azure Subscription. This option should enable the NHS to cover the CCG production instance under their existing Microsoft Support Agreement offering higher levels of support and availability from Microsoft. This option can be implemented smoothly at any time during this contract coinciding with a release upgrade to the Gateway.

Sitekit and Condatis offer to place a delivery of the CCG in ESCROW on 30th August 2024 which reflects the latest version in use within the production environment at that time. Condatis commits to maintain 1 version of the CCG within ESCROW at any time.

Q2 – Team and Implementation:

<p>Please provide pen-profiles of each team member who will be appointed to this project.</p> <p>Please make clear what expertise each identified team member will bring to this project.</p> <p>Your response should reflect skills and experience of team members relating to both the specific requirements and the general desirable attributes expressed in the specification.</p>	<p>N/A</p> <p>(Submit as attachments)</p>	<p>30%</p>
<p>Attached included with this response at Appendix A.</p>		

Classification: Official

Q3 – Risk Management:		
Please outline the risks and challenges that you foresee in delivering this contract, and your proposed approach to mitigating and or managing identified risks and challenges.	500 words	20%
Risk Management Approach Our approach to risk management is integrated across all levels, guided by our ISMS and QMS processes aligned with ISO 27001 and ISO 9001 standards. We address information security, quality, customer satisfaction, and adaptability through Agile methodologies. For compliance with Sitekit's ISMS 27001, QMS 9001 and attestation to NHS Data Security and Protection Toolkit, a periodic management review of risk and opportunities at Sitekit is required. Sitekit's MRM (Management Review Meeting) sets out the agenda and preparations needed for a management review of the combined Corporate Risks & Opportunities register (CRR).		
Risks/Challenges and Mitigation Strategies		
	Risk	Mitigation
Scale	Challenges in scaling for increased concurrent user load	Proactive monitoring of resource utilisation and application performance using Azure Monitor and Application Insights, with continuous adjustments to scale rules and application code improvements
Security	Evolution of low-security risks into broader issues	Continuous security monitoring using Azure Defender for Cloud, adopting defence in depth and zero trust strategies to enhance security posture
Availability	Not meeting the availability target of 99.5%, aspiring towards 99.9% during working hours.	Real-time monitoring with Azure Monitor, employing automatic healing strategies, direct alerts to team members, and reviewing infrastructure configurations for improved system resilience.
Disaster Recovery	Not meeting RPO and RTO objectives in a disaster	Enhancing disaster recovery planning, possibly adopting Azure Site Recovery, improving data backup and replication processes, and regular testing invocations
Transition to Multi-Tenancy Model	Architectural changes in the public beta requiring significant rework and data migration	Early tenancy architecture assessment and strategic planning of customer onboarding in the private beta
Effective Understanding and Communication of Objectives and KPIs	Challenges in effectively accessing and communicating objectives and KPIs	Collaborative access to information, enhancing communication channels for clearer understanding of the problem domain
Extraordinary Maintenance Releases	Delay in addressing urgent bug fixes	Planning for extraordinary maintenance releases for timely issue resolution.
DevOps Team Structure and Resource Prioritisation	Inadequate resource allocation in the DevOps team	Collaborative resource prioritisation based on product owner input for effective Sprint cycles.

Classification: Official

Resource Allocation and Budgeting	Ineffective resource prioritisation impacting project delivery.	Collaborative resource and budget allocation aligned with project goals
Underestimated DevOps Resource Requirement	Insufficient DevOps resources during Private Beta	Including dedicated DevOps resources in the commercial response.
Condatis Resource Integration	Integration challenges with Condatis decentralised identity specialists	Embedding Condatis resources within the team for improved collaboration
Resource Management	Delays in onboarding new resources affecting timelines	Early initiation of resource requests and maintaining strong recruitment relationships for quick access to quality candidates
Contingency Planning	Unanticipated challenges without contingency plans	Developing, evolving, and tracking project contingency plans throughout the project lifecycle

This comprehensive risk management approach ensures proactive identification and mitigation of potential challenges, aligning with industry standards and project objectives.

Q4 – Social Value:

Detail how, through the delivery of the contract, you plan to influence staff and suppliers to fight climate change through the reduction of consumption and waste.

500 words

10%

Sitekit's dedication to combatting climate change is evident in the focus on reducing carbon consumption and waste. The commitment is twofold: developing digital solutions that contribute to a more sustainable society and implementing environmentally friendly practices within their operations.

Environmental Policy

Sitekit is committed to ensuring as a business we operate in a manner that supports efforts to fight climate change through the reduction of carbon emissions and reduction of waste. As a business our technology solutions are geared towards the digitalization of services leading to overall process efficiency and a reduction in the use of paper-based systems and their associated carbon footprint.

All our IT systems are cloud based and all data centres used for data storage are carefully selected, taking into consideration the carbon offsetting commitments of those companies. Sitekit builds on the Microsoft Azure Public Cloud with Microsoft's Environmental Management System accredited to ISO 14001:2015.

At a practical level the business is committed to the principles of reduce, reuse, and recycle. We utilize suppliers who promote sustainable IT hardware and have a work from home business model which reduces our business travel impact. Where staff do have to travel for work, they are encouraged to use environmentally friendly options where practical. As a technology-based remote workforce we have very limited use of paper with the vast majority of all our work and records managed electronically. We ensure to operate in compliance with all applicable legal requirements for environmental responsibility which include the safe disposal of electrical equipment under the UK Waste Electrical and Electronic Equipment Regulations 2013.

Classification: Official

Corporate and Social Responsibility Statement.

Sitekit is committed to being a fair work employer and operates as such on a day-to-day basis. Our commitment to our staff is documented in the Employee Handbook where we communicate our values of innovation, excellence, integrity, and trust. We are an equal opportunities employer and are dedicated to inclusion and diversity which is outlined within the Employee Handbook.

We are also dedicated to our Positive Work Environment policy and the creation of a harmonious and safe working environment, which is free from harassment and bullying and in which every employee is treated with respect and dignity.

As a business, Sitekit recognizes that it has a duty to contribute positively to society and strives to achieve this through our commercial operations, where we aim to improve health care provision via digital solutions, by supporting employees with volunteer days and supporting a nominated charity. Furthermore, Sitekit is committed to promoting and providing opportunities for women in technology to help achieve gender equality in the technology sector which is a goal throughout the UK. We also consider unemployed, not in education and/or returning to the workforce applicants when recruiting new staff, to ensure there are no barriers to our employment and to provide equal opportunities to everyone.

Commercials:

Please submit your fixed price for this work. The pricing proposal must:

- (a) Supported by a comprehensive breakdown of cost, i.e., per month and allocated resources.
- (b) Be inclusive of Expenses and exclusive of VAT.

Pricing expected to be competitive within the capped budget envelope of £2m (ex VAT)

Pricing will be benchmarked against the supplier's rate card provided at G-Cloud 13.

A full breakdown of the Financials is included in Appendix B

A high-level summary of the fixed cost together with any other costs are detailed below.

Total Number of days	
Total solution Cost -	
% Discount	
Price Discount	
Final Price	£1,990,000.00

Classification: Official

The solution proposed by Sitekit will involve a team 20 members and indicative G-Cloud Rates are included below, together with indicative resource allocation.

Role	Named resource	Allocation	Rate
CEO			
CTO			
Client Operations & Security			
Service Desk Support			
Programme Manager			
Project Manager			
Product Owner			
Lead Architect			
Architect			
Lead Developer			
Developer 2			
Developer 3			
Test Lead			
Tester 2			
Tester 3			
Designer 1			
Designer 2 - Content			
Business Analyst			
Dev Ops			
Dev Ops			

Schedule 10: Request for Clarifications



Request for Clarifications

NHS Digital Staff Passport_ Technical Supplier

via G-Cloud 13

Commercial clarification questions

Reference document: **Appendix B - Question 5.xlsx**

1. Assumption tab – ID 2 NHS Authoritative Sources will work on the same principle as the Training Information System (TIS). Non NHS Authoritative Sources will be subject to separate commercial agreements.

- i) Please confirm that work to develop the DSP API is included in scope (prioritised in sprints), as well as any work by third parties to use the DSP API and integrate with the DSP (prioritised in sprints).

Sitekit Response: Sitekit confirm that work to develop the DSP API is included in scope (prioritised in sprints), as well as any work by third parties to use the DSP API and integrate with the DSP (prioritised in sprints).

2. Assumption tab – ID 15 Expectations for use with up to 100 Trusts and a total transaction capacity of 1,000,000. Transactions in production will be constrained to 1,000 per Trust per month.

- i) Please can we remove the 1,000 transactions per month in Production per trust?

Sitekit Response: Yes, we can remove the limit of 1,000 transactions per trust. Overall, there will still be a maximum limit of 1,000,000 transactions per month and, as per our latest offer:

"NHS will continue to hold 3rd party vendor licensing responsibility and receiving authorisation for those technologies are to be provided by Sitekit/ Condatis through the CCG. Any associated costs with the use of 3rd parties or specific charges associated with issuance, verification, or endorsement of Entra VC credentials received by Sitekit/ Condatis, will be passed on at cost from Sitekit to the NHS" for example Yoti.

Classification: Official

3. Condatis gateway source code

- i) Please confirm that the IP arrangements for the Condatis gateway source code remains as per the HSSF contract.

Sitekit Response:

Sitekit/ Condatis agree to make one further delivery of a Community Edition of the CCG at the end of August 2024.

- This would be based on the version of CCG in use by NHS at that point in August 2024.
- It would be delivered from Sitekit/ Condatis to NHS.
- As per the previous HSSF contract NHS would be constrained in its use by the following terms:
 - Non commercially exploitable
 - Non-transferable or sub-licensable
 - Non revokable
 - In perpetuity
 - Usable only within the Authority (NHS England) or successor organisations for the area currently covered by the Authority and only in the field of Health and Social Care.

4. Sprints and Payment schedule tab – please confirm if you would be happy to accept the following sprints and payment schedule. Reference updated UPDATED Appendix - Question 5.xlsx with tabs updated for:

- G-Cloud Cost Per month
- Sprints and Payments Schedule