



G-Cloud 14 Call-Off Contract Lot 2

This Call-Off Contract for the G-Cloud 14 Framework Agreement (RM1557.14) includes:

G-Cloud 14 Call-Off Contract

Part A: Order Form	2
Part B: Terms and conditions	27
Schedule 1: Services	50
Schedule 2: Call-Off Contract charges	51
Schedule 3: Collaboration agreement	58
Schedule 4: Alternative clause	71
Schedule 5: Guarantee	75
Schedule 6: Glossary and interpretations	84
Schedule 7: UK GDPR Information	99
Annex 1: Processing Personal Data	99
Annex 2: Joint Controller Agreement	102
Schedule 8: Corporate Resolution Planning	109
Schedule 9: Variation Form	128

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	480654931030449
Call-Off Contract reference	Buyer Ref: C351358 Supplier: [REDACTED]
Call-Off Contract title	Management Information System (Maytas) Renewal
Call-Off Contract description	Management Information system providing access and training to NHS employer-providers.
Start date	01/04/2025
Expiry date	31/03/2026
Call-Off Contract value	£35,462.99 excluding VAT
Charging method	BACS
Purchase order number	TBC

This Order Form is issued under the G-Cloud 14 Framework Agreement (RM1557.14).

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 7 - 8 Wellington Place Leeds West Yorkshire LS1 4AP
To the Supplier	Tribal Education Limited St Mary's Court, 55 St. Marys Road, Sheffield, United Kingdom, S2 4AN Company number: 04163300
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: [REDACTED]
Name: [REDACTED]
Email: [REDACTED]
Phone: [REDACTED]

For the Supplier:

Title: [REDACTED]
Name: [REDACTED]
Email: [REDACTED] and triballelegalnotices@tribalgroupp.com in relation to any notice given in accordance with this Call-Off Contract.
Phone: [REDACTED]

Call-Off Contract term

Start date	<p>This Call-Off Contract Starts on 01/04/2025 and is valid for 12 months</p> <p>The date and number of days or months is subject to clause 1.2 in Part B below.</p>
Ending (termination)	<p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least 30 Working Days from the date of written notice for undisputed sums (as per clause 18.6).</p> <p>The notice period for the Buyer is a maximum of 30 days from the date of written notice for Ending without cause (as per clause 18.1).</p>

Extension period	<p>This contract cannot be extended.</p> <p>The Parties acknowledge and agree that the Call-Off Contract shall not automatically renew.</p>
-------------------------	---

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> <p>Lot 2: Cloud software.</p>
G-Cloud Services required	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined in Schedule 1 of the Call-Off Contract.</p>
Additional Services	<p>N/A</p>
Location	<p>The Services will be delivered to remotely to NHS England.</p>
Quality Standards	<p>The quality standards required for this Call-Off Contract are those detailed in the Supplier's listing on the Framework, Agreement including the Supplier's Service definition and Supplier Terms.</p>
Technical Standards:	<p>The technical standards required for this Call-Off Contract are those detailed in the Supplier's listing on the Framework Agreement, including the Supplier's Service definition and Supplier Terms.</p>

	<p>The supplier must also maintain the following standards and certifications for the duration of this Call-Off Contract:</p> <ul style="list-style-type: none">• ISO/IEC 27001 (service security)• Cyber essentials• Cyber essentials plus
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are as detailed in the Supplier Service and Support Annexures.
Onboarding	N/A

Offboarding	N/A
Collaboration agreement	N/A

Limit on Parties' liability	<p>Defaults by either party resulting in direct loss or damage to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed [REDACTED] of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.</p> <p>The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation of or damage to any Buyer Data will not exceed or [REDACTED] of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.</p> <p>The annual total liability of the Supplier for all other Defaults will not exceed the [REDACTED] of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term.</p>
Buyer's responsibilities	<p>The Buyer is responsible for:</p> <ul style="list-style-type: none">• Using approved equipment of sufficient specification and functionality• Paying all Charges for internet access (Including data usage) charged by its internet service provider.• Meeting the Buyer's user obligations and restrictions as set out in Annex C.
Buyer's equipment	N/A

Supplier's information

Subcontractors or partners	<p>The following is a list of the Supplier's Subcontractors or Partners:</p> <p>Microsoft Azure [REDACTED] [REDACTED]</p> <p>Any Supplier Affiliate is a permitted Subcontractor.</p>
-----------------------------------	---

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 Call-Off Contract is BACS .
Payment profile	The payment profile for this Call-Off Contract is annually in advance.
Invoice details	<p>The Supplier will issue electronic invoices annually in advance. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice which includes a valid Purchase Order Number.</p> <p>All amounts stated are exclusive of VAT which shall be charged at the prevailing rate. The Buyer shall, following the Receipt of a valid VAT invoice, pay to the Supplier a sum equal to the VAT chargeable in respect of the Services.</p>
Who and where to send invoices to	<p>Invoices should clearly quote the purchase order number, be addressed to NHS England, X24 Payables K005, PO Box 312, LEEDS LS11 1HP and be sent as a PDF attachment by email to the following email address; sbs.apinvoicing@nhs.net (one invoice per PDF) and emails must not exceed 10Mb and quote, 'X24 Invoice Scanning' in subject line or alternatively invoices can be sent via post to the above address.</p> <p>Any queries regarding outstanding payments should be directed to NHS England (NHS Digital)'s Accounts Payable section by email at financialaccounts@nhs.net</p>

Invoice information required	<p>The Buyer shall issue a Purchase Order to the Supplier at the commencement of this Call-Off Contract in respect of all Services to be supplied to the Buyer under this Call-Off Contract.</p> <p>The Supplier must be in Receipt of a valid Purchase Order Number before submitting an invoice. All invoices should be sent, quoting that number to the address given on the Purchase Order. To avoid delay in payment it is important that the invoice is compliant and that it includes an item number (if applicable) and the details (name and telephone number) of the Buyer contact. Non-compliant invoices will be sent back to the Supplier, which may lead to a delay in payment.</p>
Invoice frequency	Invoice will be sent to the Buyer annually in advance.
Call-Off Contract value	Has the meaning given in Part A, above
Call-Off Contract charges	<p>The breakdown of the Charges is as set out in Order Form Schedule 2 (Call-Off Contract charges).</p> <p>Expenses are not applicable to this contract.</p> <p>Any expenses must be agreed by the Buyer in writing prior to such costs being incurred and will only be payable in accordance with the Buyer's expenses policy.</p>

Additional Buyer terms

Performance of the Service	<p>This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones:</p> <p>As set out in Schedule 1 Services.</p>
Guarantee	N/A
Warranties, representations	<p>In addition to the incorporated Framework Agreement clause 2.3, the Supplier will comply with the warranties and representations set out in the Buyer specific amendments to/refinements of the Call-Off Contract terms.</p> <p>The Supplier warrants that the Services will be provided in conformity with and meet all requirements and standards expressly set out in this Call-Off Contract.</p>
Supplemental requirements in addition to the Call-Off terms	<ol style="list-style-type: none">1. The following requirements shall take priority above all terms, conditions and specifications set out in this Call-Off Contract (including without limitation any embedded documents and terms), and the Supplier shall ensure that the software licences meet and conform with the following requirements:<ol style="list-style-type: none">1.1 The Buyer's role as national information and technology partner to the NHS and social care bodies involves the Buyer buying services for or on behalf of the NHS and social care entities. Nothing in the licences for any of the software shall have the effect of restricting the Buyer from discharging its role as the national information and technology partner for the health and care system which includes the ability of the Buyer to offer software and services to the NHS and social care entities (Specifically adhering to the permitted number of Learner Numbers/ licenced users, namely a maximum of [REDACTED] Learner Numbers and [REDACTED] licenced users).1.2 The Buyer shall be entitled to deploy the software at any location from which the Buyer is undertaking services pursuant to which the software is being licenced.

	1.3 The Supplier shall notify the Buyer in advance if any software or service permits the Supplier or any third-party remote access to the software or systems of the Buyer.					
Alternative clauses	N/A					
Buyer specific amendments to/refinements of the Call-Off Contract terms	<table><tr><td>Central Government Body</td><td>means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: a) Government Department; b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c) Non-Ministerial Department; and d) Executive Agency;</td></tr><tr><td>Cyber Security Requirements</td><td>means: a) compliance with the DSP Toolkit or any replacement of the same; b) Maintenance of Cyber Essentials and Cyber Essentials Plus Certification; and</td></tr></table>		Central Government Body	means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: a) Government Department; b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c) Non-Ministerial Department; and d) Executive Agency;	Cyber Security Requirements	means: a) compliance with the DSP Toolkit or any replacement of the same; b) Maintenance of Cyber Essentials and Cyber Essentials Plus Certification; and
Central Government Body	means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: a) Government Department; b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c) Non-Ministerial Department; and d) Executive Agency;					
Cyber Security Requirements	means: a) compliance with the DSP Toolkit or any replacement of the same; b) Maintenance of Cyber Essentials and Cyber Essentials Plus Certification; and					

		c) any other cyber security requirements relating to the Services notified to the Supplier by the Buyer from time to time;
	DSP Toolkit	means the data security and protection toolkit, an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards and supports key requirements of the GDPR, which can be accessed from https://www.dsptoolkit.nhs.uk/ , as may be amended or replaced by the Buyer or the Department of Health and Social Care from time to time;
	Project Specific IPRs	means 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 or Third Party IPRs;
	Purchase Order	means the Buyer's unique number relating to the supply of the Services;
	Receipt	means the physical or electronic arrival of the invoice at the address specified above at 'Call-Off Contract charges and payment' under the heading "Who and where to send invoices to" or at any other address given by the Buyer to the Supplier

		for the submission of invoices from time to time;
	Third Party IPRs	means any intellectual property rights owned by a third party, which are licensed by the Supplier for the purposes of providing the Services;
	Unavoidable Losses	means only the Losses specified as such in the Order Form (if any) which the Supplier may incur in the event of the Buyer ending the Call-Off Contract pursuant to Clause 18.1;
<p>1) New Clauses 11.10 to 11.14 inclusive, shall be added to Clause 11 of the Call-Off terms, as follows:</p> <p>11.10 All Project Specific IPRs shall vest in the Supplier absolutely, and the Buyer hereby assigns to the Supplier, absolutely with full title guarantee (and free from all third party rights), any and all of its right, title and interest in and to all the existing and future Project Specific IPRs, to the fullest extent permitted by law.</p> <p>11.11 Not used.</p> <p>11.12 Not used</p> <p>11.13 Each Party undertakes that it shall promptly execute all documents, make all applications, give all assistance and do or procure the doing of all acts and things as may be necessary or desirable to give full effect to the assignment of the Project Specific IPRs described in Clause 11.10 in, and to register ownership of the Project Specific IPRs in, the name of the Supplier (to the extent that registration of rights is available) and/or to give full effect to the licences granted under this Clause 11.</p> <p>11.14 The licence granted by the Supplier under Clause 11.4 shall be transferable to other Central Government Bodies.</p>		
<p>2) Clauses 18.2 and 18.3 of the Call-Off terms shall be deleted in their entirety and replaced with the following new Clauses 18.2</p>		

	<p>and 18.3:</p> <p>18.2 The Parties agree that the:</p> <ul style="list-style-type: none">• Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided• Call-Off Contract Charges paid during the notice period are reasonable compensation and cover all the Supplier's Losses, unless Unavoidable Losses are specified in the Order Form, in which case clause 18.3 shall apply to such Unavoidable Losses. <p>18.3 Subject to clause 24 (Liability), and if this clause is specified to apply in the Order Form, if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any Unavoidable Losses incurred by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Unavoidable Losses. If the Supplier has insurance, the Supplier will reduce its Unavoidable Losses by any insurance sums available. The Supplier will submit a fully itemised and costed list of the Unavoidable Losses with supporting evidence.</p> <p>3) New Clauses 4A and 4B shall be added as follows:</p> <p>4A IR35</p> <p>4A.1 This Call-Off Contract constitutes a contract for the provision of goods and/or services. Where the Supplier (or its Subcontractors) have included one or more people that are non-permanent members of staff that are not on the Supplier's (or its Subcontractors) payroll ("Contractor(s)") to fulfil its service obligations under this Call-Off Contract, the Supplier shall be fully responsible for and shall indemnify the Buyer for:</p> <ul style="list-style-type: none">• any proceedings, claims or demands by any third party (including specifically, but without limitation, HMRC and any successor, equivalent or related body pursuant to the IR35 legislation and/or any of the provisions of Income Tax Regulations);• any income tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made in connection with either the performance of the services or any payment or benefit received by the
--	---

	<p>Contractor in respect of the services, where such recovery is not prohibited by law.</p>
4A.2	The Supplier warrants that it is not, nor will it prior to the cessation of this Call-Off Contract, become a managed service company, within the meaning of section 61B of the Income Tax (Earnings and Pensions) Act 2003.
4A.3	The Supplier shall monitor the provision of the services and notify the Buyer where it considers that the activity of the Buyer may impact the Suppliers' (or its Subcontractors) IR35 Assessment in relation to the Contractors.
4B	Security of Supplier Staff
4B.1	Supplier Staff shall be subject to pre-employment checks that include, as a minimum: verification of identity, employment history, unspent criminal convictions and right to work, as detailed in the HMG Baseline Personnel Security Standard: (https://www.gov.uk/government/publications/government-baseline-personnel-security-standard), as may be amended or replaced by the Government from time to time.
4B.2	Any which require specific government National Security Vetting clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Buyer Data shall be identified and set out in the Order Form.
4B.4	All Supplier Staff that have the ability to access Buyer Data or systems holding Buyer Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.
4B.5	Where Supplier Staff are granted the ability to access Buyer Data or systems holding Buyer Data, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need such access or leave the organisation, their access rights shall be revoked within one (1) Working Day.
4)	A new Clause 16.8 shall be added as follows:
16.8	The Supplier warrants and represents that it has

	<p>complied with and throughout the Call Off Contract Period will continue to comply with the Cyber Security Requirements.</p> <p>5) Clauses 12.1 and 12.3 of the Call-Off terms and conditions shall be deleted in their entirety and replaced with the following new Clause 12.1:</p> <p>12.1 The Supplier must:</p> <ul style="list-style-type: none">• comply with the Buyer's written instructions and this Call-Off Contract when Processing any Buyer Data, including but not limited to Buyer Personal Data;• only Process the Buyer Data, including but not limited to Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body;• take reasonable steps to ensure that any Supplier Staff who have access to any Buyer Data, including but not limited to Buyer Personal Data act in compliance with Supplier's security processes. <p>12. 7 Neither Party shall do nor omit to do anything that will put the other Party in breach of the Data Protection Legislation.</p> <p>6) A new clause 7.2A shall be added to the Call-Off terms and conditions as follows:</p> <p>7.2A Electronic Invoicing</p> <p>7.2A.1 The Buyer shall accept and process for payment an electronic invoice submitted for payment by the Supplier where the invoice is undisputed and where it complies with the standard on electronic invoicing.</p> <p>7.2A.2 For the purposes of clause 7.2A.1, an electronic invoice complies with the standard on electronic invoicing where it complies with the European standard and any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870.</p> <p>7) New Clause 33.2 shall be added as follows:</p> <p>Data Protection Impact Assessment Delivery and Assistance</p>
--	---

	<p>33.2 Without limitation to the obligations as set out in Schedule 7 (UK GDPR Information), the Call-Off Contract and the Order Form, the Supplier shall participate and provide reasonable co-operation for the completion of any Data Protection Impact Assessments conducted by the Buyer relating to the Services and the deliverables. Such participation and co-operation shall include updating the Data Protection Impact Assessment at each material change of the deliverable(s) (including but not limited to each release of new software) and following any Variation.</p> <p>8) A new Clause 34 shall be added as follows:</p> <p>34 Assignment and Novation</p> <p>9) The Buyer may at its discretion assign, novate or otherwise dispose of any or all of its rights, obligations and liabilities under this Call-Off Contract and/or any associated licences to the Department of Health and Social Care, and / or any Central Government Body and the Supplier shall, at the Buyer's request, enter into an agreement in such form as the Buyer shall reasonably specify in order to enable the Buyer to exercise its rights pursuant to this clause 34 (Assignment and Novation).A new Clause 35 shall be added as follows:</p> <p>35 Subcontracts</p> <p>The Supplier shall take reasonable steps to ensure that each material Subcontract (except in the case of material Subcontract with public cloud providers) shall include:</p> <p>35.1 a right under the Contracts (Rights of Third Parties) Act 1999 for the Buyer to enforce any provisions under the material Subcontract which confer a benefit upon the Buyer;</p> <p>35.2 a provision enabling the Buyer to enforce the material Subcontract as if it were the Supplier; and</p> <p>35.3 obligations no less onerous on the Subcontractor than those imposed on the Supplier under this Call-Off Contract.</p> <p>10) A new Clause 36 shall be added as follows:</p> <p>36 Execution and Counterparts</p> <p>36.1 This Call-Off Contract may be executed in any number of counterparts (including by electronic transmission), each of</p>
--	---

	<p>which when executed shall constitute an original but all counterparts together shall constitute one and the same instrument.</p> <p>36.2 Execution of this Call-Off Contract may be carried out in accordance with the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (SI 2016/696) and the Electronic Communications Act 2000. In the event each Party agrees to sign this Call-Off Contract by electronic signature (whatever form the electronic signature takes) it is confirmed that this method of signature is as conclusive of each Party's intention to be bound by this Call-Off Contract as if signed by each Party's manuscript signature. In such situation, this Call-Off Contract shall be formed on the date on which both Parties have electronically signed the Call-Off Contract as recorded in the Buyer's electronic contract management system.</p> <p>11) Schedule 7 - Processing Data (Framework Agreement)</p> <p>12.1) For the purposes of incorporating Schedule 7 of the Framework Agreement into this Call-Off Contract, paragraph 5(d) shall be deleted in its entirety and replaced with the following:</p> <p>(d) not transfer Personal Data outside of the UK</p> <p>(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;</p> <p>(ii) the Data Subject has enforceable rights and effective legal remedies;</p> <p>(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and</p> <p>(iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data.</p>
--	--

Personal Data and Data Subjects	Schedule 7 is being used: Annex 1.
Intellectual Property	IPR provisions are outlined in the section 11 of the call off terms.
Social Value	N/A
Performance Indicators	Data supplied by the Supplier in relation to Performance Indicators is deemed the Intellectual Property of the Buyer and may be published by the Buyer.

1. Formation of contract

1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off 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 clauses 8.3 to 8.6 inclusive of the Framework Agreement.

2. Background to the agreement

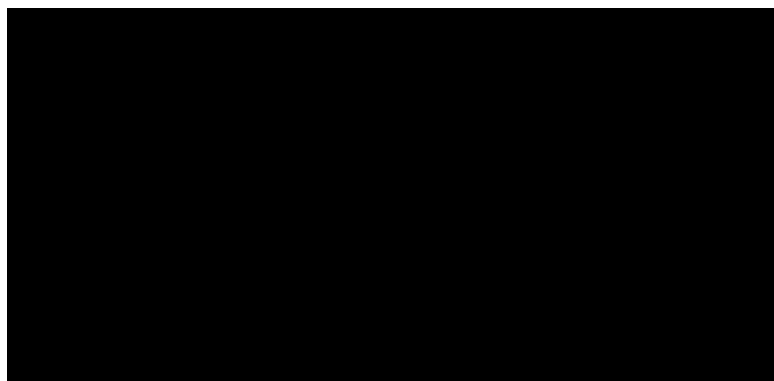
2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.14.

Signatures:

Tribal Education Limited – St Mary's Court, 55 St. Marys Road,
Sheffield, United Kingdom, S2 4AN

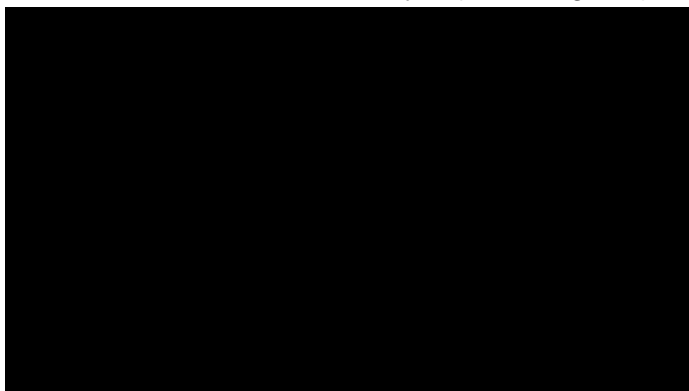
Company number: **04163300**

For and on behalf of the Supplier (Tribal Education Limited)

A large black rectangular redaction box covering the signature area for Tribal Education Limited.

NHS England - 7 & 8 Wellington Place Leeds, West Yorkshire Leeds
LS1 4AP

For and on behalf of the Buyer (NHS England)

A large black rectangular redaction box covering the signature area for NHS England.

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

Buyer Benefits

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

[G-Cloud 14 Buyer 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 36 months.

2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses, schedules 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)

5.4 to 5.6 (Change of control)

5.7 (Fraud)

5.8 (Notice of fraud)

7 (Transparency and Audit)

8.3 to 8.6 (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)
30 (Insurance)
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

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

a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'

a reference to 'CCS' or to 'CCS and/or the Buyer' will be a reference to 'the Buyer'

a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

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.

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

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 14 digit 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

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 trademarks 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:

alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;

alleging that the Buyer Data violates, infringes or misappropriate any rights of a third party;
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 judgement 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:

rights granted to the Buyer under this Call-Off Contract

Supplier's performance of the Services

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:

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

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

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:

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

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-security-classifications>

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: <https://www.npsa.gov.uk/content/adopt-risk-management-approach> and Protection of Sensitive Information and Assets: <https://www.npsa.gov.uk/sensitive-information-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/technologycode-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:

return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it

return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer

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

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

work with the Buyer on any ongoing work

return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

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.

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 CDDO 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 Neither Party will be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Call-Off Contract (other than a payment of money) to the extent that such delay or failure is a result of a Force Majeure event.

23.2A Party will promptly (on becoming aware of the same) notify the other Party of a Force Majeure event or potential Force Majeure event which could affect its ability to perform its obligations under this Call-Off Contract.

23.3 Each Party will use all reasonable endeavours to continue to perform its obligations under the Call-Off Contract and to mitigate the effects of Force Majeure. If a Force Majeure event prevents a Party from performing its obligations under the Call-Off Contract for more than 30 consecutive Working Days, the other Party can End the Call-Off Contract with immediate effect by notice in writing.

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 is not a 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.

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.

The Supplier will cooperate 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.

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

- its failure to comply with the provisions of this clause

- 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

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

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 using the template in Schedule 9 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 using the template in Schedule 9. 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 Call-Off 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

1.1 This Call-Off Contract is for the provision of Maytas only, unless otherwise expressly varied otherwise in writing by agreement of the contracting Parties;

1.2 The Software modules and Specifications are detailed in Annex A.

1.3 Tribal will provide the Customer with the Software, the Software Service, Type of Support Services and Service Levels as detailed below:

Table 1: Software, Software Service, Support Services and Service Level

Software	Software Service	Type of Support Services	Service Level
Maytas	Tribal Cloud SaaS	Core Support Services (Annex D.1)*;	Not applicable
		Tribal Support Services (Annex D.2)*	Not applicable
		Tribal Cloud SaaS (Annex D.3)*	Enhanced

*These constitute the Supplier Service and Support Annexures.

1.4 The Service Levels (SLA) are as set out in Supplier Service and Support Annexures.

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:

1 **Fees and Payment Terms Overview**

The Buyer shall pay Supplier the Fees in accordance with the provisions set out in this Schedule 2, the Payment Terms, and on the terms and conditions of this Call-Off Contract in British Pounds, on the Due Date, without any set off, withholding or deduction whatsoever.

2 **Annual Subscription Fees** - The total Annual Subscription Fee for the period 01 April 2025 to 31 March 2026 is £35,462.99 (as set out in Table 2B below). The actual Charges will be determined by applying any adjustment required due to Learner Numbers falling within a new Metric Band (if applicable). Where applicable, the parties will enter into a variation in accordance with Part B Clause 32, Variation Process to record increased Annual Subscription Fees as a result of changes to the required Learner Numbers Metric Band.

3 Expenses claimed by the supplier are not applicable to this contract.

Table 2B: Annual Subscription Fees

Dates	Total Annual Subscription Fee	Services and usage
1 April 2025 to 31 March 2026	£35,462.99 excluding VAT	<ul style="list-style-type: none">Software as detailed in Annex ATribal Support and Tribal Cloud Services (as detailed in Annexures D.1, D.2 and D.3)Fees cover usage:-<ul style="list-style-type: none">[REDACTED] Maytas Licenced Users[REDACTED] Learner Numbers*
Total	£35,462.99 Excluding VAT	

*Additional Learner Numbers are priced [REDACTED]
[REDACTED] he Buyer will promptly inform the Supplier if its Learner Numbers exceed the level detailed in Table 2B and will pay for additional usage in line with the terms of this Schedule 2.

4 **Payment Terms** - The Fees will be paid in accordance with the Payment Terms in Table 2C below.

Table 2C: Payment Terms

Fee	Due Date
Annual Subscription Fee	Annually in advance, due 30 days after the receipt of an invoice, with the first payment due on the Start Date.

5 Definitions

The Definitions applicable to this Schedule 2 are detailed below:

Definitions	<ul style="list-style-type: none">• Due Date: as defined in section Error! Reference source not found., of this Schedule 2.• Fees: means Charges• Learner Number: the number of Permitted Users (namely, learners) for the Buyer for a twelve month period;• Permitted Users: the users or groups of users permitted by the Buyer to access and utilise the functionality of the Software and/or Software Service, for example, enrolled students and Learners of the Buyer;• Software: the specified software provided by Supplier;• Software Service: the applicable service used by the Buyer to access the specified Software, e.g. Tribal Cloud SaaS;
-------------	---

Schedule 3: Collaboration agreement (Not Used)

This agreement is made on [enter date]

between:

[Buyer name] of [Buyer address] (the Buyer)

[Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

[Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

[Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

[Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address]

[Company name] a company incorporated in [company address] under [registration number], whose registered office is at [registered address] together (the Collaboration Suppliers and each of them a Collaboration Supplier).

Whereas the:

Buyer and the Collaboration Suppliers have entered into the Call-Off Contracts (defined below) for the provision of various IT and telecommunications (ICT) services
Collaboration Suppliers now wish to provide for the ongoing cooperation of the Collaboration Suppliers in the provision of services under their respective Call-Off Contract to the Buyer

In consideration of the mutual covenants contained in the Call-Off Contracts and this Agreement and intending to be legally bound, the parties agree as follows:

1. Definitions and interpretation

1.1 As used in this Agreement, the capitalised expressions will have the following meanings unless the context requires otherwise:

1.1.1 "Agreement" means this collaboration agreement, containing the Clauses and Schedules

1.1.2 "Call-Off Contract" means each contract that is let by the Buyer to one of the Collaboration Suppliers

1.1.3 "Contractor's Confidential Information" has the meaning set out in the Call-Off Contracts

- 1.1.4 "Confidential Information" means the Buyer Confidential Information or any Collaboration Supplier's Confidential Information
- 1.1.5 "Collaboration Activities" means the activities set out in this Agreement
- 1.1.6 "Buyer Confidential Information" has the meaning set out in the Call-Off Contract
- 1.1.7 "Default" means any breach of the obligations of any Collaboration Supplier or any Default, act, omission, negligence or statement of any Collaboration Supplier, its employees, servants, agents or subcontractors in connection with or in relation to the subject matter of this Agreement and in respect of which such Collaboration Supplier is liable (by way of indemnity or otherwise) to the other parties
- 1.1.8 "Detailed Collaboration Plan" has the meaning given in clause 3.2
- 1.1.9 "Dispute Resolution Process" means the process described in clause 9
- 1.1.10 "Effective Date" means [insert date]
- 1.1.11 "Force Majeure Event" has the meaning given in clause 11.1.1
- 1.1.12 "Mediator" has the meaning given to it in clause 9.3.1
- 1.1.13 "Outline Collaboration Plan" has the meaning given to it in clause 3.1
- 1.1.14 "Term" has the meaning given to it in clause 2.1
- 1.1.15 "Working Day" means any day other than a Saturday, Sunday or public holiday in England and Wales

1.2 General

- 1.2.1 As used in this Agreement the:
 - 1.2.1.1 masculine includes the feminine and the neuter
 - 1.2.1.2 singular includes the plural and the other way round
 - 1.2.1.3 A reference to any statute, enactment, order, regulation or other similar instrument will be viewed as a reference to the statute, enactment, order, regulation or instrument as amended by any subsequent statute, enactment, order, regulation or instrument or as contained in any subsequent reenactment.
- 1.2.2 Headings are included in this Agreement for ease of reference only and will not affect the interpretation or construction of this Agreement.

- 1.2.3 References to Clauses and Schedules are, unless otherwise provided, references to clauses of and schedules to this Agreement.
- 1.2.4 Except as otherwise expressly provided in this Agreement, all remedies available to any party under this Agreement are cumulative and may be exercised concurrently or separately and the exercise of any one remedy will not exclude the exercise of any other remedy.
- 1.2.5 The party receiving the benefit of an indemnity under this Agreement will use its reasonable endeavours to mitigate its loss covered by the indemnity.

2. Term of the agreement

- 2.1 This Agreement will come into force on the Effective Date and, unless earlier terminated in accordance with clause 10, will expire 6 months after the expiry or termination (however arising) of the exit period of the last Call-Off Contract (the "Term").
- 2.2 A Collaboration Supplier's duty to perform the Collaboration Activities will continue until the end of the exit period of its last relevant Call-Off Contract.

3. Provision of the collaboration plan

- 3.1 The Collaboration Suppliers will, within 2 weeks (or any longer period as notified by the Buyer in writing) of the Effective Date, provide to the Buyer detailed proposals for the Collaboration Activities they require from each other (the "Outline Collaboration Plan").
- 3.2 Within 10 Working Days (or any other period as agreed in writing by the Buyer and the Collaboration Suppliers) of [receipt of the proposals] or [the Effective Date], the Buyer will prepare a plan for the Collaboration Activities (the "Detailed Collaboration Plan"). The Detailed Collaboration Plan will include full details of the activities and interfaces that involve all of the Collaboration Suppliers to ensure the receipt of the services under each Collaboration Supplier's respective [contract] [Call-Off Contract], by the Buyer. The Detailed Collaboration Plan will be based on the Outline Collaboration Plan and will be submitted to the Collaboration Suppliers for approval.
- 3.3 The Collaboration Suppliers will provide the help the Buyer needs to prepare the Detailed Collaboration Plan.
- 3.4 The Collaboration Suppliers will, within 10 Working Days of receipt of the Detailed Collaboration Plan, either:
 - 3.4.1 approve the Detailed Collaboration Plan
 - 3.4.2 reject the Detailed Collaboration Plan, giving reasons for the rejection

- 3.5 The Collaboration Suppliers may reject the Detailed Collaboration Plan under clause 3.4.2 only if it is not consistent with their Outline Collaboration Plan in that it imposes additional, more onerous, obligations on them.
- 3.6 If the parties fail to agree the Detailed Collaboration Plan under clause 3.4, the dispute will be resolved using the Dispute Resolution Process.

4. Collaboration activities

- 4.1 The Collaboration Suppliers will perform the Collaboration Activities and all other obligations of this Agreement in accordance with the Detailed Collaboration Plan.
- 4.2 The Collaboration Suppliers will provide all additional cooperation and assistance as is reasonably required by the Buyer to ensure the continuous delivery of the services under the Call-Off Contract.
- 4.3 The Collaboration Suppliers will ensure that their respective subcontractors provide all cooperation and assistance as set out in the Detailed Collaboration Plan.

5. Invoicing

- 5.1 If any sums are due under this Agreement, the Collaboration Supplier responsible for paying the sum will pay within 30 Working Days of receipt of a valid invoice.
- 5.2 Interest will be payable on any late payments under this Agreement under the Late Payment of Commercial Debts (Interest) Act 1998, as amended.

6. Confidentiality

- 6.1 Without prejudice to the application of the Official Secrets Acts 1911 to 1989 to any Confidential Information, the Collaboration Suppliers acknowledge that any Confidential Information obtained from or relating to the Crown, its servants or agents is the property of the Crown.
- 6.2 Each Collaboration Supplier warrants that:
 - 6.2.1 any person employed or engaged by it (in connection with this Agreement in the course of such employment or engagement) will only use Confidential Information for the purposes of this Agreement

- 6.2.2 any person employed or engaged by it (in connection with this Agreement) will not disclose any Confidential Information to any third party without the prior written consent of the other party
- 6.2.3 it will take all necessary precautions to ensure that all Confidential Information is treated as confidential and not disclosed (except as agreed) or used other than for the purposes of this Agreement by its employees, servants, agents or subcontractors
- 6.2.4 neither it nor any person engaged by it, whether as a servant or a consultant or otherwise, will use the Confidential Information for the solicitation of business from the other or from the other party's servants or consultants or otherwise
- 6.3 The provisions of clauses 6.1 and 6.2 will not apply to any information which is:
 - 6.3.1 or becomes public knowledge other than by breach of this clause 6
 - 6.3.2 in the possession of the receiving party without restriction in relation to disclosure before the date of receipt from the disclosing party
 - 6.3.3 received from a third party who lawfully acquired it and who is under no obligation restricting its disclosure
 - 6.3.4 independently developed without access to the Confidential Information
 - 6.3.5 required to be disclosed by law or by any judicial, arbitral, regulatory or other authority of competent jurisdiction
- 6.4 The Buyer's right, obligations and liabilities in relation to using and disclosing any Collaboration Supplier's Confidential Information provided under this Agreement and the Collaboration Supplier's right, obligations and liabilities in relation to using and disclosing any of the Buyer's Confidential Information provided under this Agreement, will be as set out in the [relevant contract] [Call-Off Contract].

7. Warranties

- 7.1 Each Collaboration Supplier warrants and represents that:
 - 7.1.1 it has full capacity and authority and all necessary consents (including but not limited to, if its processes require, the consent of its parent company) to enter into and to perform this Agreement and that this Agreement is executed by an authorised representative of the Collaboration Supplier
 - 7.1.2 its obligations will be performed by appropriately experienced, qualified and trained personnel with all due skill, care and diligence including but not limited to good

industry practice and (without limiting the generality of this clause 7) in accordance with its own established internal processes

- 7.2 Except as expressly stated in this Agreement, all warranties and conditions, whether express or implied by statute, common law or otherwise (including but not limited to fitness for purpose) are excluded to the extent permitted by law.

8. Limitation of liability

- 8.1 None of the parties exclude or limit their liability for death or personal injury resulting from negligence, or for any breach of any obligations implied by Section 2 of the Supply of Goods and Services Act 1982.
- 8.2 Nothing in this Agreement will exclude or limit the liability of any party for fraud or fraudulent misrepresentation.
- 8.3 Subject always to clauses 8.1 and 8.2, the liability of the Buyer to any Collaboration Suppliers for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of statutory duty or otherwise under this Agreement (excluding Clause 6.4, which will be subject to the limitations of liability set out in the relevant Contract) will be limited to [(£,000)].
- 8.4 Subject always to clauses 8.1 and 8.2, the liability of each Collaboration Supplier for all claims (by way of indemnity or otherwise) arising whether in contract, tort (including negligence), misrepresentation (other than if made fraudulently), breach of statutory duty or otherwise under this Agreement will be limited to [Buyer to specify].
- 8.5 Subject always to clauses 8.1, 8.2 and 8.6 and except in respect of liability under clause 6 (excluding clause 6.4, which will be subject to the limitations of liability set out in the [relevant contract] [Call-Off Contract]), in no event will any party be liable to any other for:
- 8.5.1 indirect loss or damage
 - 8.5.2 special loss or damage
 - 8.5.3 consequential loss or damage
 - 8.5.4 loss of profits (whether direct or indirect)
 - 8.5.5 loss of turnover (whether direct or indirect)
 - 8.5.6 loss of business opportunities (whether direct or indirect)
 - 8.5.7 damage to goodwill (whether direct or indirect)
- 8.6 Subject always to clauses 8.1 and 8.2, the provisions of clause 8.5 will not be taken as limiting the right of the Buyer to among other things, recover as a direct loss any:
- 8.6.1 additional operational or administrative costs and expenses arising from a Collaboration Supplier's Default

8.6.2 wasted expenditure or charges rendered unnecessary or incurred by the Buyer arising from a Collaboration Supplier's Default

9. Dispute resolution process

- 9.1 All disputes between any of the parties arising out of or relating to this Agreement will be referred, by any party involved in the dispute, to the representatives of the parties specified in the Detailed Collaboration Plan.
- 9.2 If the dispute cannot be resolved by the parties' representatives nominated under clause 9.1 within a maximum of 5 Working Days (or any other time agreed in writing by the parties) after it has been referred to them under clause 9.1, then except if a party seeks urgent injunctive relief, the parties will refer it to mediation under the process set out in clause 9.3 unless the Buyer considers (acting reasonably and considering any objections to mediation raised by the other parties) that the dispute is not suitable for resolution by mediation.
- 9.3 The process for mediation and consequential provisions for mediation are:
 - 9.3.1 a neutral adviser or mediator will be chosen by agreement between the parties or, if they are unable to agree upon a Mediator within 10 Working Days after a request by one party to the other parties to appoint a Mediator or if the Mediator agreed upon is unable or unwilling to act, any party will within 10 Working Days from the date of the proposal to appoint a Mediator or within 10 Working Days of notice to the parties that he is unable or unwilling to act, apply to the President of the Law Society to appoint a Mediator
 - 9.3.2 the parties will within 10 Working Days of the appointment of the Mediator meet to agree a programme for the exchange of all relevant information and the structure of the negotiations
 - 9.3.3 unless otherwise agreed by the parties in writing, all negotiations connected with the dispute and any settlement agreement relating to it will be conducted in confidence and without prejudice to the rights of the parties in any future proceedings
 - 9.3.4 if the parties reach agreement on the resolution of the dispute, the agreement will be put in writing and will be binding on the parties once it is signed by their authorised representatives
 - 9.3.5 failing agreement, any of the parties may invite the Mediator to provide a non binding but informative opinion in writing. The opinion will be provided on a without prejudice basis and will not be used in evidence in any proceedings relating to this Agreement without the prior written consent of all the parties

9.3.6 if the parties fail to reach agreement in the structured negotiations within 20 Working Days of the Mediator being appointed, or any longer period the parties agree on, then any dispute or difference between them may be referred to the courts

9.4 The parties must continue to perform their respective obligations under this Agreement and under their respective Contracts pending the resolution of a dispute.

10. Termination and consequences of termination

10.1 Termination

10.1.1 The Buyer has the right to terminate this Agreement at any time by notice in writing to the Collaboration Suppliers whenever the Buyer has the right to terminate a Collaboration Supplier's [respective contract] [Call-Off Contract].

10.1.2 Failure by any of the Collaboration Suppliers to comply with their obligations under this Agreement will constitute a Default under their [relevant contract] [Call-Off Contract]. In this case, the Buyer also has the right to terminate by notice in writing the participation of any Collaboration Supplier to this Agreement and sever its name from the list of Collaboration Suppliers, so that this Agreement will continue to operate between the Buyer and the remaining Collaboration Suppliers.

10.2 Consequences of termination

10.2.1 Subject to any other right or remedy of the parties, the Collaboration Suppliers and the Buyer will continue to comply with their respective obligations under the [contracts] [Call-Off Contracts] following the termination (however arising) of this Agreement.

10.2.2 Except as expressly provided in this Agreement, termination of this Agreement will be without prejudice to any accrued rights and obligations under this Agreement.

11. General provisions

11.1 Force majeure

11.1.1 For the purposes of this Agreement, the expression "Force Majeure Event" will mean any cause affecting the performance by a party of its obligations under this Agreement arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control, including acts of God, riots, war or armed conflict, acts of terrorism, acts of government, local government or Regulatory Bodies, fire, flood, storm or earthquake, or disaster but excluding any industrial dispute relating to any party, the party's personnel or any other failure of a Subcontractor.

11.1.2 Subject to the remaining provisions of this clause 11.1, any party to this Agreement may claim relief from liability for non-performance of its obligations to the extent this is due to a Force Majeure Event.

11.1.3 A party cannot claim relief if the Force Majeure Event or its level of exposure to the event is attributable to its wilful act, neglect or failure to take reasonable precautions against the relevant Force Majeure Event.

11.1.4 The affected party will immediately give the other parties written notice of the Force Majeure Event. The notification will include details of the Force Majeure Event together with evidence of its effect on the obligations of the affected party, and any action the affected party proposes to take to mitigate its effect.

11.1.5 The affected party will notify the other parties in writing as soon as practicable after the Force Majeure Event ceases or no longer causes the affected party to be unable to comply with its obligations under this Agreement. Following the notification, this Agreement will continue to be performed on the terms existing immediately before the Force Majeure Event unless agreed otherwise in writing by the parties.

11.2 Assignment and subcontracting

11.2.1 Subject to clause 11.2.2, the Collaboration Suppliers will not assign, transfer, novate, sub-license or declare a trust in respect of its rights under all or a part of this Agreement or the benefit or advantage without the prior written consent of the Buyer.

11.2.2 Any subcontractors identified in the Detailed Collaboration Plan can perform those elements identified in the Detailed Collaboration Plan to be performed by the Subcontractors.

11.3 Notices

11.3.1 Any notices given under or in relation to this Agreement will be deemed to have been properly delivered if sent by recorded or registered post or by fax and will be deemed for the purposes of this Agreement to have been given or made at the time the letter would, in the ordinary course of post, be delivered or at the time shown on the sender's fax transmission report.

11.3.2 For the purposes of clause 11.3.1, the address of each of the parties are those in the Detailed Collaboration Plan.

11.4 Entire agreement

11.4.1 This Agreement, together with the documents and agreements referred to in it, constitutes the entire agreement and understanding between the parties in respect of the matters dealt with in it and supersedes any previous agreement between the Parties about this.

11.4.2 Each of the parties agrees that in entering into this Agreement and the documents and agreements referred to in it does not rely on, and will have no remedy in respect of, any statement, representation, warranty or undertaking (whether negligently or innocently made) other than as expressly set out in this Agreement. The only remedy available to each party in respect of any statements, representation, warranty or understanding will be for breach of contract under the terms of this Agreement.

11.4.3 Nothing in this clause 11.4 will exclude any liability for fraud.

11.5 Rights of third parties

Nothing in this Agreement will grant any right or benefit to any person other than the parties or their respective successors in title or assignees, or entitle a third party to enforce any provision and the parties do not intend that any term of this Agreement should be enforceable by a third party by virtue of the Contracts (Rights of Third Parties) Act 1999.

11.6 Severability

If any provision of this Agreement is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, that provision will be severed without effect to the remaining provisions. If a provision of this Agreement that is fundamental to the accomplishment of the purpose of this Agreement is held to any extent to be invalid, the parties will immediately commence good faith negotiations to remedy that invalidity.

11.7 Variations

No purported amendment or variation of this Agreement or any provision of this Agreement will be effective unless it is made in writing by the parties.

11.8 No waiver

The failure to exercise, or delay in exercising, a right, power or remedy provided by this Agreement or by law will not constitute a waiver of that right, power or remedy. If a party waives a breach of any provision of this Agreement this will not operate as a waiver of a subsequent breach of that provision, or as a waiver of a breach of any other provision.

11.9 Governing law and jurisdiction

This Agreement will be governed by and construed in accordance with English law and without prejudice to the Dispute Resolution Process, each party agrees to submit to the exclusive jurisdiction of the courts of England and Wales.

Executed and delivered as an agreement by the parties or their duly authorised attorneys the day and year first above written.

For and on behalf of the Buyer

Signed by:

Full name (capitals):

Position:

Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position

: Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position

: Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position

: Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position

: Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position

: Date:

For and on behalf of the [Company name]

Signed by:

Full name (capitals):

Position:

Date:

Collaboration Agreement Schedule 1: List of contracts

Collaboration supplier	Name/reference of contract	Effective date of contract

Collaboration Agreement Schedule 2 [Insert Outline Collaboration Plan]

Schedule 4: Alternative clauses (Not Used)

1. Introduction

- 1.1 This Schedule specifies the alternative clauses that may be requested in the Order Form and, if requested in the Order Form, will apply to this Call-Off Contract.

2. Clauses selected

- 2.1 The Buyer may, in the Order Form, request the following alternative Clauses:

2.1.1 Scots Law and Jurisdiction

- 2.1.2 References to England and Wales in incorporated Framework Agreement clause 15.1 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.

- 2.1.3 Reference to England and Wales in Working Days definition within the Glossary and interpretations section will be replaced with Scotland.

- 2.1.4 References to the Contracts (Rights of Third Parties) Act 1999 will be removed in clause 27.1. Reference to the Freedom of Information Act 2000 within the defined terms for 'FOIA/Freedom of Information Act' to be replaced with Freedom of Information (Scotland) Act 2002.

- 2.1.5 Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.1.

- 2.1.6 References to "tort" will be replaced with "delict" throughout

- 2.2 The Buyer may, in the Order Form, request the following Alternative Clauses:

- 2.2.1 Northern Ireland Law (see paragraph 2.3, 2.4, 2.5, 2.6 and 2.7 of this Schedule)

2.3 Discrimination

- 2.3.1 The Supplier will comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular the:

Employment (Northern Ireland) Order 2002

Fair Employment and Treatment (Northern Ireland) Order 1998

Sex Discrimination (Northern Ireland) Order 1976 and 1988

Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003

Equal Pay Act (Northern Ireland) 1970

Disability Discrimination Act 1995

Race Relations (Northern Ireland) Order 1997

Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996

Employment Equality (Age) Regulations (Northern Ireland) 2006

Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000

Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002
 The Disability Discrimination (Northern Ireland) Order 2006
 The Employment Relations (Northern Ireland) Order 2004
 Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006
 Employment Relations (Northern Ireland) Order 2004
 Work and Families (Northern Ireland) Order 2006

and will use its best endeavours to ensure that in its employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract it promotes equality of treatment and opportunity between:

persons of different religious beliefs or political opinions
 men and women or married and unmarried persons
 persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)
 persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)
 persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)
 persons of different ages
 persons of differing sexual orientation

2.3.2 The Supplier will take all reasonable steps to secure the observance of clause 2.3.1 of this Schedule by all Supplier Staff.

2.4 Equality policies and practices

2.4.1 The Supplier will introduce and will procure that any Subcontractor will also introduce and implement an equal opportunities policy in accordance with guidance from and to the satisfaction of the Equality Commission. The Supplier will review these policies on a regular basis (and will procure that its Subcontractors do likewise) and the Buyer will be entitled to receive upon request a copy of the policy.

2.4.2 The Supplier will take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in clause 2.3 above). These steps will include:

the issue of written instructions to staff and other relevant persons
 the appointment or designation of a senior manager with responsibility for equal opportunities
 training of all staff and other relevant persons in equal opportunities and harassment matters
 the inclusion of the topic of equality as an agenda item at team, management and staff meetings

The Supplier will procure that its Subcontractors do likewise with their equal opportunities policies.

2.4.3 The Supplier will inform the Buyer as soon as possible in the event of:

the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its Subcontractors during the Call-Off Contract Term by any Industrial or Fair Employment Tribunal or court,

The Supplier will take any necessary steps (including the dismissal or replacement of any relevant staff or Subcontractor(s)) as the Buyer directs and will seek the advice of the Equality Commission in order to prevent any offence or repetition of the unlawful discrimination as the case may be.

2.4.4 The Supplier will monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and will provide an annual report on the composition of the workforce and applicants to the Buyer. If the monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier will review the operation of its relevant policies and take positive action if appropriate. The Supplier will impose on its Subcontractors obligations similar to those undertaken by it in this clause 2.4 and will procure that those Subcontractors comply with their obligations.

2.4.5 The Supplier will provide any information the Buyer requests (including Information requested to be provided by any Subcontractors) for the purpose of assessing the Supplier's compliance with its obligations under clauses 2.4.1 to 2.4.5 of this Schedule.

2.5 Equality

2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

2.5.2 The Supplier acknowledges that the Buyer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours to assist (and to ensure that relevant Subcontractor helps) the Buyer in relation to same.

2.6 Health and safety

2.6.1 The Supplier will promptly notify the Buyer of any health and safety hazards which may arise in connection with the performance of its obligations under the Call-Off Contract. The Buyer will promptly notify the Supplier of any health and safety hazards which may exist or arise at the Buyer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Contract.

- 2.6.2 While on the Buyer premises, the Supplier will comply with any health and safety measures implemented by the Buyer in respect of Supplier Staff and other persons working there.
- 2.6.3 The Supplier will notify the Buyer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Buyer premises if that incident causes any personal injury or damage to property which could give rise to personal injury.
- 2.6.4 The Supplier will comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other persons working on the Buyer premises in the performance of its obligations under the Call-Off Contract.
- 2.6.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Buyer on request.

2.7 Criminal damage

- 2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Buyer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Buyer under any insurance policy).
- 2.7.2 If during the Call-Off Contract Term any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.
- 2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Buyer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Buyer's cost and the Supplier will (at no additional cost to the Buyer) provide any help the Buyer reasonably requires with the appeal.
- 2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

Schedule 5: Guarantee (Not Used)

[A Guarantee should only be requested if the Supplier's financial standing is not enough on its own to guarantee delivery of the Services. This is a draft form of guarantee which can be used to procure a Call Off Guarantee, and so it will need to be amended to reflect the Beneficiary's requirements]

This deed of guarantee is made on [insert date, month, year] between:

(1) [Insert the name of the Guarantor] a company incorporated in England and Wales with number [insert company number] whose registered office is at [insert details of the guarantor's registered office] [or a company incorporated under the Laws of [insert country], registered in [insert country] with number [insert number] at [insert place of registration], whose principal office is at [insert office details]]('Guarantor'); in favour of
and

(2) The Buyer whose offices are [insert Buyer's official address]
('Beneficiary') **Whereas:**

The guarantor has agreed, in consideration of the Buyer entering into the Call-Off Contract with the Supplier, to guarantee all of the Supplier's obligations under the Call-Off Contract.

It is the intention of the Parties that this document be executed and take effect as a deed.

[Where a deed of guarantee is required, include the wording below and populate the box below with the guarantor company's details. If a deed of guarantee isn't needed then the section below and other references to the guarantee should be deleted.

Suggested headings are as follows:

- Demands and notices
- Representations and Warranties
- Obligation to enter into a new Contract
- Assignment
- Third Party Rights
- Governing Law
- This Call-Off Contract is conditional upon the provision of a Guarantee to the Buyer from the guarantor in respect of the Supplier.

Guarantor company	[Enter Company name] 'Guarantor'
-------------------	----------------------------------

Guarantor company address	[Enter Company address]
Account manager	[Enter Account Manager name]
	Address: [Enter Account Manager address]
	Phone: [Enter Account Manager phone number]
	Email: [Enter Account Manager email]
	Fax: [Enter Account Manager fax if applicable]

In consideration of the Buyer entering into the Call-Off Contract, the Guarantor agrees with the Buyer as follows:

Definitions and interpretation

In this Deed of Guarantee, unless defined elsewhere in this Deed of Guarantee or the context requires otherwise, defined terms will have the same meaning as they have for the purposes of the Call-Off Contract.

Term	Meaning
Call-Off Contract	Means [the Guaranteed Agreement] made between the Buyer and the Supplier on [insert date].
Guaranteed Obligations	Means all obligations and liabilities of the Supplier to the Buyer under the Call-Off Contract together with all obligations owed by the Supplier to the Buyer that are supplemental to, incurred under, ancillary to or calculated by reference to the Call-Off Contract.
Guarantee	Means the deed of guarantee described in the Order Form (Parent Company Guarantee).

References to this Deed of Guarantee and any provisions of this Deed of Guarantee or to any other document or agreement (including to the Call-Off Contract) apply now, and as amended, varied, restated, supplemented, substituted or novated in the future.

Unless the context otherwise requires, words importing the singular are to include the plural and vice versa.

References to a person are to be construed to include that person's assignees or transferees or successors in title, whether direct or indirect.

The words 'other' and 'otherwise' are not to be construed as confining the meaning of any following words to the class of thing previously stated if a wider construction is possible.

Unless the context otherwise requires:

reference to a gender includes the other gender and the neuter

references to an Act of Parliament, statutory provision or statutory instrument also apply if amended, extended or re-enacted from time to time

any phrase introduced by the words 'including', 'includes', 'in particular', 'for example' or similar, will be construed as illustrative and without limitation to the generality of the related general words

References to Clauses and Schedules are, unless otherwise provided, references to Clauses of and Schedules to this Deed of Guarantee.

References to liability are to include any liability whether actual, contingent, present or future.

Guarantee and indemnity

The Guarantor irrevocably and unconditionally guarantees that the Supplier duly performs all of the guaranteed obligations due by the Supplier to the Buyer.

If at any time the Supplier will fail to perform any of the guaranteed obligations, the Guarantor irrevocably and unconditionally undertakes to the Buyer it will, at the cost of the Guarantor:

fully perform or buy performance of the guaranteed obligations to the Buyer

as a separate and independent obligation and liability, compensate and keep the Buyer compensated against all losses and expenses which may result from a failure by the Supplier to perform the guaranteed obligations under the Call-Off Contract

As a separate and independent obligation and liability, the Guarantor irrevocably and unconditionally undertakes to compensate and keep the Buyer compensated on demand against all losses and expenses of whatever nature, whether arising under statute, contract or at common Law, if any obligation guaranteed by the guarantor is or becomes unenforceable, invalid or illegal as if the obligation guaranteed had not become unenforceable, invalid or illegal provided that the guarantor's liability will be no greater than the Supplier's liability would have been if the obligation guaranteed had not become unenforceable, invalid or illegal.

Obligation to enter into a new contract

If the Call-Off Contract is terminated or if it is disclaimed by a liquidator of the Supplier or the obligations of the Supplier are declared to be void or voidable, the Guarantor will, at the request of the Buyer, enter into a Contract with the Buyer in the same terms as the Call-Off Contract and the obligations of the Guarantor under such substitute agreement will be the same as if the Guarantor had been original obligor under the Call-Off Contract or under an agreement entered into on the same terms and at the same time as the Call-Off Contract with the Buyer.

Demands and notices

Any demand or notice served by the Buyer on the Guarantor under this Deed of Guarantee will be in writing, addressed to:

[Enter Address of the Guarantor in England and Wales]

[Enter Email address of the Guarantor

representative] For the Attention of **[insert details]**

or such other address in England and Wales as the Guarantor has notified the Buyer in writing as being an address for the receipt of such demands or notices.

Any notice or demand served on the Guarantor or the Buyer under this Deed of Guarantee will be deemed to have been served if:

delivered by hand, at the time of delivery
posted, at 10am on the second Working Day after it was put into the post

sent by email, at the time of despatch, if despatched before 5pm on any Working Day, and in any other case at 10am on the next Working Day

In proving Service of a notice or demand on the Guarantor or the Buyer, it will be sufficient to prove that delivery was made, or that the envelope containing the notice or demand was properly addressed and posted as a prepaid first class recorded delivery letter, or that the fax message was properly addressed and despatched.

Any notice purported to be served on the Buyer under this Deed of Guarantee will only be valid when received in writing by the Buyer.

Beneficiary's protections

The Guarantor will not be discharged or released from this Deed of Guarantee by:

any arrangement made between the Supplier and the Buyer (whether or not such arrangement is made with the assent of the Guarantor)
any amendment to or termination of the Call-Off Contract
any forbearance or indulgence as to payment, time, performance or otherwise granted by the Buyer (whether or not such amendment, termination, forbearance or indulgence is made with the assent of the Guarantor)
the Buyer doing (or omitting to do) anything which, but for this provision, might exonerate the Guarantor

This Deed of Guarantee will be a continuing security for the Guaranteed Obligations and accordingly:

it will not be discharged, reduced or otherwise affected by any partial performance (except to the extent of such partial performance) by the Supplier of the Guaranteed Obligations or by any omission or delay on the part of the Buyer in exercising its rights under this Deed of Guarantee

it will not be affected by any dissolution, amalgamation, reconstruction, reorganisation, change in status, function, control or ownership, insolvency, liquidation, administration, appointment of a receiver, voluntary arrangement, any legal limitation or other incapacity, of the Supplier, the Buyer, the Guarantor or any other person

if, for any reason, any of the Guaranteed Obligations is void or unenforceable against the Supplier, the Guarantor will be liable for that purported obligation or liability as if the same were fully valid and enforceable and the Guarantor were principal debtor the rights of the Buyer against the Guarantor under this Deed of Guarantee are in addition to, will not be affected by and will not prejudice, any other security, guarantee, indemnity or other rights or remedies available to the Buyer

The Buyer will be entitled to exercise its rights and to make demands on the Guarantor under this Deed of Guarantee as often as it wishes. The making of a demand (whether effective, partial or defective) relating to the breach or non-performance by the Supplier of any Guaranteed Obligation will not preclude the Buyer from making a further demand relating to the same or some other Default regarding the same Guaranteed Obligation.

The Buyer will not be obliged before taking steps to enforce this Deed of Guarantee against the Guarantor to:

obtain judgement against the Supplier or the Guarantor or any third party in any court
make or file any claim in a bankruptcy or liquidation of the Supplier or any third party
take any action against the Supplier or the Guarantor or any third party
resort to any other security or guarantee or other means of payment

No action (or inaction) by the Buyer relating to any such security, guarantee or other means of payment will prejudice or affect the liability of the Guarantor.

The Buyer's rights under this Deed of Guarantee are cumulative and not exclusive of any rights provided by Law. The Buyer's rights may be exercised as often as the Buyer deems expedient. Any waiver by the Buyer of any terms of this Deed of Guarantee, or of any Guaranteed Obligations, will only be effective if given in writing and then only for the purpose and upon the terms and conditions on which it is given.

Any release, discharge or settlement between the Guarantor and the Buyer will be conditional upon no security, disposition or payment to the Buyer by the Guarantor or any other person being void, set aside or ordered to be refunded following any enactment or Law relating to liquidation, administration or insolvency or for any other reason. If such condition will not be fulfilled, the Buyer will be entitled to enforce this Deed of Guarantee subsequently as if such release, discharge or settlement had not occurred and any such payment had not been made. The Buyer will be entitled to retain this security before and after the payment, discharge or satisfaction of all monies, obligations and liabilities that are or may become due owing or incurred to the Buyer from the Guarantor for such period as the Buyer may determine.

Representations and warranties

The Guarantor hereby represents and warrants to the Buyer that:

the Guarantor is duly incorporated and is a validly existing company under the Laws of its place of incorporation
has the capacity to sue or be sued in its own name

the Guarantor has power to carry on its business as now being conducted and to own its Property and other assets

the Guarantor has full power and authority to execute, deliver and perform its obligations under this Deed of Guarantee and no limitation on the powers of the Guarantor will be exceeded as a result of the Guarantor entering into this Deed of Guarantee

the execution and delivery by the Guarantor of this Deed of Guarantee and the performance by the Guarantor of its obligations under this Deed of Guarantee including entry into and performance of a Call-Off Contract following Clause 3) have been duly authorised by all necessary corporate action and do not contravene or conflict with:

- the Guarantor's memorandum and articles of association or other equivalent constitutional documents, any existing Law, statute, rule or Regulation or any judgement, decree or permit to which the Guarantor is subject
- the terms of any agreement or other document to which the Guarantor is a party or which is binding upon it or any of its assets
- all governmental and other authorisations, approvals, licences and consents, required or desirable

This Deed of Guarantee is the legal valid and binding obligation of the Guarantor and is enforceable against the Guarantor in accordance with its terms.

Payments and set-off

All sums payable by the Guarantor under this Deed of Guarantee will be paid without any set-off, lien or counterclaim, deduction or withholding, except for those required by Law. If any deduction or withholding must be made by Law, the Guarantor will pay that additional amount to ensure that the Buyer receives a net amount equal to the full amount which it would have received if the payment had been made without the deduction or withholding.

The Guarantor will pay interest on any amount due under this Deed of Guarantee at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgement.

The Guarantor will reimburse the Buyer for all legal and other costs (including VAT) incurred by the Buyer in connection with the enforcement of this Deed of Guarantee.

Guarantor's acknowledgement

The Guarantor warrants, acknowledges and confirms to the Buyer that it has not entered into this

Deed of Guarantee in reliance upon the Buyer nor been induced to enter into this Deed of Guarantee by any representation, warranty or undertaking made by, or on behalf of the Buyer, (whether express or implied and whether following statute or otherwise) which is not in this Deed of Guarantee.

Assignment

The Buyer will be entitled to assign or transfer the benefit of this Deed of Guarantee at any time to any person without the consent of the Guarantor being required and any such assignment or transfer will not release the Guarantor from its liability under this Guarantee.

The Guarantor may not assign or transfer any of its rights or obligations under this Deed of Guarantee.

Severance

If any provision of this Deed of Guarantee is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision will be severed and the remainder of the provisions will continue in full force and effect as if this Deed of Guarantee had been executed with the invalid, illegal or unenforceable provision eliminated.

Third-party rights

A person who is not a Party to this Deed of Guarantee will have no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Deed of Guarantee. This Clause does not affect any right or remedy of any person which exists or is available otherwise than following that Act.

Governing law

This Deed of Guarantee, and any non-Contractual obligations arising out of or in connection with it, will be governed by and construed in accordance with English Law.

The Guarantor irrevocably agrees for the benefit of the Buyer that the courts of England will have jurisdiction to hear and determine any suit, action or proceedings and to settle any dispute which may arise out of or in connection with this Deed of Guarantee and for such purposes hereby irrevocably submits to the jurisdiction of such courts.

Nothing contained in this Clause will limit the rights of the Buyer to take proceedings against the Guarantor in any other court of competent jurisdiction, nor will the taking of any such proceedings in one or more jurisdictions preclude the taking of proceedings in any other jurisdiction, whether concurrently or not (unless precluded by applicable Law).

The Guarantor irrevocably waives any objection which it may have now or in the future to the courts of England being nominated for this Clause on the ground of venue or otherwise and agrees not to claim that any such court is not a convenient or appropriate forum.

[The Guarantor hereby irrevocably designates, appoints and empowers **[enter the Supplier name]** [or a suitable alternative to be agreed if the Supplier's registered office is not in England or Wales] either at its registered office or on fax number **[insert fax number]** from time to time to act as its authorised agent to receive notices, demands, Service of process and any other legal summons in England and Wales for the purposes of any legal action or proceeding brought or to be brought by the Buyer in respect of this Deed of Guarantee. The Guarantor hereby irrevocably consents to the Service of notices and demands, Service of process or any other legal summons served in such way.]

IN WITNESS whereof the Guarantor has caused this instrument to be executed and delivered as a Deed the day and year first before written.

EXECUTED as a DEED by

[Insert name of the Guarantor] acting by **[Insert names]**

Director

Director/Secretary

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> <p>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> <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	Data, Personal Data and any information, which may include (but isn't limited to) any: 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: 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> <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	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: https://www.gov.uk/guidance/check-employment-status-fortax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Financial Metrics	The following financial and accounting measures: Dun and Bradstreet score of 50 Operating Profit Margin of 2% Net Worth of 0 Quick Ratio of 0.7

Force Majeure	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any: 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> <p>The following do not constitute a Force Majeure event: 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> <p>Majeure at the time this Call-Off Contract was entered into 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</p>
Former Supplier	<p>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).</p>
Framework Agreement	<p>The clauses of framework agreement RM1557.14 together with the Framework Schedules.</p>
Fraud	<p>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.</p>

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: a voluntary arrangement a winding-up petition the appointment of a receiver or administrator an unresolved statutory demand a Schedule A1 moratorium a Supplier Trigger Event
Intellectual Property Rights or IPR	Intellectual Property Rights are: (a) 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 (b) 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 (c) 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: the supplier's own limited company a service or a personal service company a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
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, judgement 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, judgement, 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.
Performance Indicators	The performance information required by the Buyer from the Supplier set out in the Order Form.
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> <p>induce that person to perform improperly a relevant function or activity</p> <p>reward that person for improper performance of a relevant function or activity</p> <p>commit any offence:</p> <p>under the Bribery Act 2010</p> <p>under legislation creating offences concerning Fraud</p> <p>at common Law concerning Fraud</p> <p>committing or attempting or conspiring to commit Fraud</p>

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 high performance 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 G-Cloud Services, including backup data and Performance Indicators 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 G-Cloud 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.
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.
Trigger Event	The Supplier simultaneously fails to meet three or more Financial Metrics for a period of at least ten Working Days.
Variation	This has the meaning given to it in clause 32 (Variation process).
Variation Impact Assessment	<p>An assessment of the impact of a variation request by the Buyer completed in good faith, including:</p> <p>details of the impact of the proposed variation on the Deliverables and the Supplier's ability to meet its other obligations under the Call-Off Contract;</p> <p>details of the cost of implementing the proposed variation;</p> <p>details of the ongoing costs required by the proposed variation when implemented, including any increase or decrease in the Charges, any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party;</p> <p>a timetable for the implementation, together with any proposals for the testing of the variation; and</p> <p>such other information as the Buyer may reasonably request in (or in response to) the variation request;</p>

Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Intentionally Blank

Schedule 7: UK GDPR Information

This schedule reproduces the annexes to the UK GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract and clause and schedule references are to those in the Framework Agreement but references to CCS have been amended

Annex 1 - Processing Personal Data

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

1.1.1.1 The contact details of the Buyer's Data Protection Officer are: [REDACTED] - england.dpo@nhs.net

1.1.1.2 The contact details of the Supplier's Data Protection Officer are: [REDACTED] - DataPrivacy@tribalgroupp.com

1.1.1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.1.1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller and Processor for each Category of Personal Data	<p>The Buyer is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:</p> <p>The following Learner details:</p> <ul style="list-style-type: none">• First name• Last name• NI Number,• Gender• Date of birth• Ethnic group• Address,• Telephone number• Mobile number• Email address• Unique learner number• Learning difficulty/learning disability,• Prior attainment level plus other non-personal fields relating to learner's apprenticeship. <p>The Parties are Independent Controllers of Personal Data</p> <p><i>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:</i></p> <ul style="list-style-type: none">• <i>Business contact details of Supplier Personnel for which the Supplier is the Controller,</i>

	<ul style="list-style-type: none"> • <i>Business contact details of any directors, officers, employees, agents, consultants and contractors of the Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under the Framework Agreement) for which the Buyer is the Controller,</i>
Duration of the Processing	<i>For the duration of the Call-Off Contract</i>
Nature and purposes of the Processing	<p>Collecting these fields is a contractual requirement of the Education, Skills Funding Agency placed on apprenticeship providers that use the Maytas system including NHSE.</p> <p>The nature of the processing is:</p> <ul style="list-style-type: none"> • Collection • Storage • Duplication • Electronic viewing • Deletion and destruction of data.
Type of Personal Data	<p>The following Learner details:</p> <ul style="list-style-type: none"> • Title • First name • Last name • Position • NI Number, • Gender • Date of birth • Ethnic group • Address, • Telephone number • Mobile number • Email address • Unique learner number • Learning difficulty/learning disability, • Prior attainment level plus other non-personal fields relating to learner's apprenticeship.
Categories of Data Subject	Students / Apprentices trained by NHS Organisations

International transfers and legal gateway	The Supplier's customer hosting services for Maytas are outsourced to its business partner Microsoft. Personal data is stored in Microsoft's UK Datacentre (MS-South).
Plan for return and destruction of the data once the Processing is complete	<ul style="list-style-type: none">• At the end of the Call-Off Contract Term the Buyer shall specify the data to be deleted and to returned by written notification• Where 'deleted', Supplier to confirm deletion in writing no later than 30 days after the Buyer's notification• Where 'returned', the Supplier to provide the data by secure means in a format which supports effective migration to a new platform employing commonly used means• Where the Supplier wishes to 'preserve', Supplier notifies the Buyer of the legal provisions being relied upon through written notification.

Annex 2 - Joint Controller Agreement (Not Used)

Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2 to 15 of Schedule 7 (Where one Party is Controller and the other Party is Processor) and paragraphs 17 to 27 of Schedule 7 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [select: Supplier or Buyer]:

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

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

2. Undertakings of both Parties

1.1.2.1 The Supplier and Buyer each undertake that they shall:

- (a) report to the other Party every [x] months on:
 - (i) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);
 - (ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

- (iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;
 - (iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
 - (v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law, that it has received in relation to the subject matter of the Framework Agreement during that period;
- (b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
- (c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
- (d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Framework Agreement or is required by Law) that disclosure or transfer of Personal Data is otherwise considered to be lawful processing of that Personal Data in accordance with Article 6 of the UK GDPR or EU GDPR (as the context requires). For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;
- (e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;
- (f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
- (g) use all reasonable endeavours to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
 - (i) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;
 - (ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and
 - (iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

- (h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Personal Data Breach;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
- (i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and
- (j) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.
- (k) where the Personal Data is subject to UK GDPR, not transfer such Personal Data outside of the UK unless the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:
 - (i) the destination country has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR or DPA 2018 Section 74; or
 - (ii) the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75) as agreed with the non-transferring Party which could include relevant parties entering into the International Data Transfer Agreement (the “**IDTA**”), or International Data Transfer Agreement Addendum to the European Commission’s SCCs (“the **Addendum**”), as published by the Information Commissioner’s Office from time to time, as well as any additional measures;
 - (iii) the Data Subject has enforceable rights and effective legal remedies;
 - (iv) the transferring Party complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and
 - (v) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data; and
- (l) where the Personal Data is subject to EU GDPR, not transfer such Personal Data outside of the EU unless the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:
 - (i) the transfer is in accordance with Article 45 of the EU GDPR; or

- (ii) the transferring Party has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the non-transferring Party which could include relevant parties entering into Standard Contractual Clauses in the European Commission's decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time as well as any additional measures;
- (iii) the Data Subject has enforceable rights and effective legal remedies;
- (iv) the transferring Party complies with its obligations under EU GDPR by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and
- (v) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data.

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

3. Data Protection Breach

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

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

Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

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

- (a) the nature of the Personal Data Breach;
- (b) the nature of Personal Data affected;
- (c) the categories and number of Data Subjects concerned;
- (d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;
- (e) measures taken or proposed to be taken to address the Personal Data Breach; and
- (f) describe the likely consequences of the Personal Data Breach.

4. Audit

1.1.4.1 The Supplier shall permit:

- (a) The Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or
- (b) The Buyer, or a third-party auditor acting under the Buyer's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Framework Agreement, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

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

5. Impact Assessments

1.1.5.1 The Parties shall:

provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Framework Agreement, in accordance with the terms of Article 30 UK GDPR.

6. ICO Guidance

The Parties agree to take account of any non-mandatory guidance issued by the Information Commissioner, any relevant Central Government Body and/or any other regulatory authority. The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the Framework Agreement to ensure that it complies with any guidance issued by the Information Commissioner, any relevant Central Government Body and/or any other regulatory authority.

7. Liabilities for Data Protection Breach

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

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

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

if no view as to responsibility is expressed by the Information Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the procedure set out in clause 32 of the Framework Agreement (Managing disputes).

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

the liability will be apportioned between the Parties in accordance with the decision of the Court.

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

- (a) if the Buyer is responsible for the relevant Personal Data Breach, then the Buyer shall be responsible for the Claim Losses;
- (b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and
- (c) if responsibility for the relevant Personal Data Breach is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.

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

8. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Buyer shall be entitled to terminate the Framework Agreement by issuing a Termination Notice to the Supplier in accordance with Clause 5.1.

9. Sub-Processing

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

- (a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Framework Agreement, and provide evidence of such due diligence to the other Party where reasonably requested; and
- (b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

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

Schedule 8 (Corporate Resolution Planning)

Definitions

In this Schedule, the following words shall have the following meanings and they shall supplement Schedule 6 (Glossary and interpretations):

"Accounting Reference Date"	means in each year the date to which the Supplier prepares its annual audited financial statements;
"Annual Revenue"	<p>means, for the purposes of determining whether an entity is a Public Sector Dependent Supplier, the audited consolidated aggregate revenue (including share of revenue of joint ventures and Associates) reported by the Supplier or, as appropriate, the Supplier Group in its most recent published accounts, subject to the following methodology:</p> <p>figures for accounting periods of other than 12 months should be scaled pro rata to produce a proforma figure for a 12 month period; and</p> <p>where the Supplier, the Supplier Group and/or their joint ventures and Associates report in a foreign currency, revenue should be converted to</p>

	British Pound Sterling at the closing exchange rate on the Accounting Reference Date;
“Appropriate Authority” or “Appropriate Authorities”	means the Buyer and the Cabinet Office Markets and Suppliers Team or, where the Supplier is a Strategic Supplier, the Cabinet Office Markets and Suppliers Team;
“Associates”	means, in relation to an entity, an undertaking in which the entity owns, directly or indirectly, between 20% and 50% of the voting rights and exercises a degree of control sufficient for the undertaking to be treated as an associate under generally accepted accounting principles;
"Cabinet Office Markets and Suppliers Team"	means the UK Government's team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function;

“Class 1 Transaction”	has the meaning set out in the listing rules issued by the UK Listing Authority;
“Control”	the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “Controls” and “Controlled” shall be interpreted accordingly;
“Corporate Change Event”	<p>means:</p> <p>any change of Control of the Supplier or a Parent Undertaking of the Supplier;</p> <p>any change of Control of any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Services;</p> <p>any change to the business of the Supplier or any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Services;</p> <p>a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the London Stock Exchange plc;</p> <p>an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking place in respect of the Supplier or any Parent Undertaking of the Supplier;</p> <p>payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the Net Asset Value of the Supplier or the ultimate Parent Undertaking of</p>

	<p>the Supplier Group respectively in any 12 month period;</p> <p>an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group;</p> <p>any member of the Supplier Group stopping payment of its debts generally or becoming unable to pay its debts within the meaning of section 123(1) of the Insolvency Act 1986 or any member of the Supplier Group ceasing to carry on all or substantially all its business, or any compromise, composition, arrangement or agreement being made with creditors of any member of the Supplier Group;</p> <p>the appointment of a receiver, administrative receiver or administrator in respect of or over all or a material part of the undertaking or assets of any member of the Supplier Group; and/or</p> <p>any process or events with an effect analogous to those in paragraphs (e) to (g) inclusive above occurring to a member of the Supplier Group in a jurisdiction outside England and Wales;</p>
"Corporate Change Event Grace Period"	<p>means a grace period agreed to by the Appropriate Authority for providing CRP Information and/or updates to Business Continuity Plan after a Corporate Change Event;</p>
"Corporate Resolvability Assessment (Structural Review)"	<p>means part of the CRP Information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraph 3 and Annex 2 of this Schedule;</p>

<p>“Critical National Infrastructure” or “CNI”</p>	<p>means those critical elements of UK national infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:</p> <p>major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or</p> <p>significant impact on the national security, national defence, or the functioning of the UK;</p>
<p>“Critical Service Contract”</p>	<p>means the overall status of the Services provided under the Call-Off Contract as determined by the Buyer and specified in Paragraph 2 of this Schedule;</p>
<p>“CRP Information”</p>	<p>means the corporate resolution planning information, together, the:</p> <p>(a) Exposure Information (Contracts List);</p> <p>(b) Corporate Resolvability Assessment (Structural Review); and</p> <p>(c) Financial Information and Commentary</p>

“Dependent Parent Undertaking”	means any Parent Undertaking which provides any of its Subsidiary Undertakings and/or Associates, whether directly or indirectly, with any financial, trading, managerial or other assistance of whatever nature, without which the Supplier would be unable to continue the day to day conduct and operation of its business in the same manner as carried on at the time of entering into the Call-Off Contract, including for the avoidance of doubt the provision of the Services in accordance with the terms of the Call-Off Contract;
“FDE Group” “Financial Distress Event”	<p>means the [Supplier, Subcontractors, [the Guarantor]</p> <p>the credit rating of an FDE Group entity dropping below the applicable Financial Metric;</p> <p>an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;</p> <p>there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity;</p> <p>an FDE Group entity committing a material breach of covenant to its lenders;</p> <p>a Subcontractor notifying CCS or the Buyer that the Supplier has not satisfied any material sums properly due under a specified invoice and not subject to a genuine dispute;</p>

	<p>any of the following:</p> <p>commencement of any litigation against an FDE Group entity with respect to financial indebtedness greater than £5m or obligations under a service contract with a total contract value greater than £5m;</p> <p>non-payment by an FDE Group entity of any financial indebtedness;</p> <p>any financial indebtedness of an FDE Group entity becoming due as a result of an event of default;</p> <p>the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity;</p> <p>or</p> <p>the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity;</p> <p>in each case which the Buyer reasonably believes (or would be likely to reasonably believe) could directly impact on the continued performance and delivery of the Services in accordance with the Call-Off Contract; and</p> <p>any two of the Financial Metrics for the Supplier not being met at the same time.</p>
“Parent Undertaking”	has the meaning set out in section 1162 of the Companies Act 2006;
“Public Sector Dependent Supplier”	means a supplier where that supplier, or that supplier’s group has Annual Revenue of £50 million or more of which over 50% is generated from UK Public Sector Business;

“Strategic Supplier”	means those suppliers to government listed at https://www.gov.uk/government/publications/strategic-suppliers ;
“Subsidiary Undertaking”	has the meaning set out in section 1162 of the Companies Act 2006;
“Supplier Group”	means the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings;
“UK Public Sector Business”	means any goods, service or works provision to UK public sector bodies, including Central Government Departments and their arm's length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police, fire and rescue, education bodies and devolved administrations; and

“UK Public Sector / CNI Contract Information”	means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 3 to 5 and Annex 1;
--	---

Service Status and Supplier Status

This Call-Off Contract ‘is not’ a Critical Service Contract.

The Supplier shall notify the Buyer and the Cabinet Office Markets and Suppliers Team in writing within 5 Working Days of the Start Date and throughout the Call-Off Contract Term within 120 days after each Accounting Reference Date as to whether or not it is a Public Sector Dependent Supplier. The contact email address for the Markets and Suppliers Team is resolution.planning@cabinetoffice.gov.uk.

The Buyer and the Supplier recognise that, where specified in the Framework Agreement, CCS shall have the right to enforce the Buyer's rights under this Schedule.

Provision of Corporate Resolution Planning Information

Paragraphs 3 to 5 shall apply if the Call-Off Contract has been specified as a Critical Service Contract under Paragraph 2.1 or the Supplier is or becomes a Public Sector Dependent Supplier.

Subject to Paragraphs 3.6, 3.10 and 3.11:

where the Call-Off Contract is a Critical Service Contract, the Supplier shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the Start Date; and

except where it has already been provided, where the Supplier is a Public Sector Dependent Supplier, it shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the date of the Appropriate Authority's or Appropriate Authorities' request.

The Supplier shall ensure that the CRP Information provided pursuant to Paragraphs 3.2, 3.8 and 3.9:

is full, comprehensive, accurate and up to date;

is split into three parts:

Exposure Information (Contracts List);

Corporate Resolvability Assessment (Structural Review);

Financial Information and Commentary

and is structured and presented in accordance with the requirements and explanatory notes set out in the latest published version of the Resolution Planning Guidance Note published by the Cabinet Office Government Commercial Function and available at

<https://www.gov.uk/government/publications/the-sourcing-and-consultancy-playbooks> and contains the level of detail required (adapted as necessary to the Supplier's circumstances);

incorporates any additional commentary, supporting documents and evidence which would reasonably be required by the Appropriate Authority or Appropriate Authorities to understand and consider the information for approval;

provides a clear description and explanation of the Supplier Group members that have agreements for goods, services or works provision in respect of UK Public Sector Business and/or Critical National Infrastructure and the nature of those agreements; and

complies with the requirements set out at Annex 1 (Exposure Information (Contracts List)), Annex 2 (Corporate Resolvability Assessment (Structural Review)) and Annex 3 (Financial Information and Commentary) respectively.

Following receipt by the Appropriate Authority or Appropriate Authorities of the CRP Information pursuant to Paragraphs 3.2, 3.8 and 3.9, the Buyer shall procure that the Appropriate Authority or Appropriate Authorities shall discuss in good faith the contents of the CRP Information with the Supplier and no later than 60 days after the date on which the CRP Information was delivered by the Supplier either provide an Assurance to the Supplier that the Appropriate Authority or Appropriate Authorities approve the CRP Information or that the Appropriate Authority or Appropriate Authorities reject the CRP Information.

If the Appropriate Authority or Appropriate Authorities reject the CRP Information:

the Buyer shall (and shall procure that the Cabinet Office Markets and Suppliers Team shall) inform the Supplier in writing of its reasons for its rejection; and

the Supplier shall revise the CRP Information, taking reasonable account of the Appropriate Authority's or Appropriate Authorities' comments, and shall re-submit the CRP Information to the Appropriate Authority or Appropriate Authorities for approval within 30 days of the date of the Appropriate Authority's or Appropriate Authorities' rejection. The provisions of paragraph 3.3 to 3.5 shall apply again to any resubmitted CRP Information provided that

either Party may refer any disputed matters for resolution under clause 32 of the Framework Agreement (Managing disputes).

Where the Supplier or a member of the Supplier Group has already provided CRP Information to a central government body or the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely to the Cabinet Office Markets and Suppliers Team) and has received an Assurance of its CRP Information from that central government body and the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely from the Cabinet Office Markets and Suppliers Team), then provided that the Assurance remains Valid (which has the meaning in paragraph 3.7 below) on the date by which the CRP Information would otherwise be required, the Supplier shall not be required to provide the CRP Information under Paragraph 3.2 if it provides a copy of the Valid Assurance to the Appropriate Authority or Appropriate Authorities on or before the date on which the CRP Information would otherwise have been required.

An Assurance shall be deemed Valid for the purposes of Paragraph 3.6 if:

the Assurance is within the validity period stated in the Assurance (or, if no validity period is stated, no more than 12 months has elapsed since it was issued and no more than 18 months has elapsed since the Accounting Reference Date on which the CRP Information was based); and

no Corporate Change Events or Financial Distress Events (or events which would be deemed to be Corporate Change Events or Financial Distress Events if the Call-Off Contract had then been in force) have occurred since the date of issue of the Assurance.

If the Call-Off Contract is a Critical Service Contract, the Supplier shall provide an updated version of the CRP Information (or, in the case of Paragraph 3.8.3 of its initial CRP Information) to the Appropriate Authority or Appropriate Authorities:

within 14 days of the occurrence of a Financial Distress Event (along with any additional highly confidential information no longer exempted from disclosure under Paragraph 3.11) unless the Supplier is relieved of the consequences of the Financial Distress Event as a result of credit ratings being revised upwards;

within 30 days of a Corporate Change Event unless

the Supplier requests and the Appropriate Authority (acting reasonably) agrees to a Corporate Change Event Grace Period, in the event of which the time period for the Supplier to comply with this Paragraph shall be extended as determined by the Appropriate Authority (acting reasonably) but shall in any case be no longer than six months after the Corporate Change Event. During a Corporate Change Event Grace Period the Supplier shall regularly and fully engage with the Appropriate Authority to enable it to understand the nature of the Corporate Change Event and the Appropriate Authority shall reserve the right to terminate a Corporate Change Event Grace Period at any time if the Supplier fails to comply with this Paragraph; or

not required pursuant to Paragraph 3.10;

within 30 days of the date that:

the credit rating(s) of each of the Supplier and its Parent Undertakings fail to meet any of the criteria specified in Paragraph 3.10; or

none of the credit rating agencies specified at Paragraph 3.10 hold a public credit rating for the Supplier or any of its Parent Undertakings; and

in any event, within 6 months after each Accounting Reference Date or within 15 months of the date of the previous Assurance received from the Appropriate Authority (whichever is the earlier), unless:

updated CRP Information has been provided under any of Paragraphs 3.8.1 3.8.2 or 3.8.3 since the most recent Accounting Reference Date (being no more than 12 months previously) within the timescales that would ordinarily be required for the provision of that information under this Paragraph 3.8.4; or

not required pursuant to Paragraph 3.10.

Where the Supplier is a Public Sector Dependent Supplier and the Call-Off Contract is not a Critical Service Contract, then on the occurrence of any of the events specified in Paragraphs 3.8.1 to 3.8.4, the Supplier shall provide at the request of the Appropriate Authority or Appropriate Authorities and within the applicable timescales for each event as set out in Paragraph 3.8 (or such longer timescales as may be notified to the Supplier by the Buyer), the CRP Information to the Appropriate Authority or Appropriate Authorities.

Where the Supplier or a Parent Undertaking of the Supplier has a credit rating of either:

Aa3 or better from Moody's;

AA- or better from Standard and Poors;

AA- or better from Fitch;

the Supplier will not be required to provide any CRP Information unless or until either (i) a Financial Distress Event occurs (unless the Supplier is relieved of the consequences of the Financial Distress Event due to credit ratings being revised upwards) or (ii) the Supplier and its Parent Undertakings cease to fulfil the criteria set out in this Paragraph 3.10, in which cases the

Supplier shall provide the updated version of the CRP Information in accordance with paragraph 3.8.

Subject to Paragraph 5, where the Supplier demonstrates to the reasonable satisfaction of the Appropriate Authority or Appropriate Authorities that a particular item of CRP Information is highly confidential, the Supplier may, having orally disclosed and discussed that information with the Appropriate Authority or Appropriate Authorities, redact or omit that information from the CRP Information provided that if a Financial Distress Event occurs, this exemption shall no longer apply and the Supplier shall promptly provide the relevant information to the Appropriate Authority or Appropriate Authorities to the extent required under Paragraph 3.8.

Termination Rights

The Buyer shall be entitled to terminate the Call-Off Contract if the Supplier is required to provide CRP Information under Paragraph 3 and either:

the Supplier fails to provide the CRP Information within 4 months of the Start Date if this is a Critical Service Contract or otherwise within 4 months of the Appropriate Authority's or Appropriate Authorities' request; or

the Supplier fails to obtain an Assurance from the Appropriate Authority or Appropriate Authorities within 4 months of the date that it was first required to provide the CRP Information under the Call-Off Contract, which shall be deemed to be an event to which Clause 18.4 applies.

Confidentiality and usage of CRP Information

The Buyer agrees to keep the CRP Information confidential and use it only to understand the implications of an Insolvency Event of the Supplier and/or Supplier Group members on its UK Public Sector Business and/or services in respect of CNI and to enable contingency planning to maintain service continuity for end users and protect CNI in such eventuality.

Where the Appropriate Authority is the Cabinet Office Markets and Suppliers Team, at the Supplier's request, the Buyer shall use reasonable endeavours to procure that the Cabinet Office enters into a confidentiality and usage agreement with the Supplier containing terms no less stringent than those placed on the Buyer under paragraph 5.1 and incorporated Framework Agreement clause 34.

The Supplier shall use reasonable endeavours to obtain consent from any third party which has restricted the disclosure of the CRP Information to enable disclosure of that information to the Appropriate Authority or Appropriate Authorities pursuant to Paragraph 3 subject, where necessary, to the Appropriate Authority or Appropriate Authorities entering into an appropriate confidentiality agreement in the form required by the third party.

Where the Supplier is unable to procure consent pursuant to Paragraph 5.3, the Supplier shall use all reasonable endeavours to disclose the CRP Information to the fullest extent possible by limiting the amount of information it withholds including by:

redacting only those parts of the information which are subject to such obligations of confidentiality;

providing the information in a form that does not breach its obligations of confidentiality including (where possible) by:

summarising the information;

grouping the information;

anonymising the information; and

presenting the information in general terms

The Supplier shall provide the Appropriate Authority or Appropriate Authorities with contact details of any third party which has not provided consent to disclose CRP Information where that third party is also a public sector body and where the Supplier is legally permitted to do so.

ANNEX 1: EXPOSURE: CRITICAL CONTRACTS LIST

The Supplier shall:

provide details of all agreements held by members of the Supplier Group where those agreements are for goods, services or works provision and:

are with any UK public sector bodies including: central government departments and their arms-length bodies and agencies, non-departmental public bodies, NHS bodies, local buyers, health bodies, police fire and rescue, education bodies and the devolved administrations;

are with any private sector entities where the end recipient of the service, goods or works provision is any of the bodies set out in Paragraph 1.1(a) of this Annex 1 and where the member of the Supplier Group is acting as a key sub-contractor under the contract with the end recipient; or

involve or could reasonably be considered to involve CNI;

provide the Appropriate Authority with a copy of the latest version of each underlying contract worth more than £5m per contract year and their related key sub-contracts, which shall be included as embedded documents within the CRP Information or via a directly accessible link

ANNEX 2: CORPORATE RESOLVABILITY ASSESSMENT (STRUCTURAL REVIEW)

The Supplier shall:

provide sufficient information to allow the Appropriate Authority to understand the implications on the Supplier Group's UK Public Sector Business and CNI agreements listed pursuant to Annex 1 if the Supplier or another member of the Supplier Group is subject to an Insolvency Event;

ensure that the information is presented so as to provide a simple, effective and easily understood overview of the Supplier Group; and

provide full details of the importance of each member of the Supplier Group to the Supplier Group's UK Public Sector Business and CNI agreements listed pursuant to Annex 1 and the dependencies between each.

ANNEX 3: Financial information AND COMMENTARY

The Supplier shall:

provide sufficient financial information for the Supplier Group level, contracting operating entities level, and shared services entities' level to allow the Appropriate Authority to understand the current financial interconnectedness of the Supplier Group and the current performance of the Supplier as a standalone entity; and

ensure that the information is presented in a simple, effective and easily understood manner.

For the avoidance of doubt the financial information to be provided pursuant to Paragraph 1 of this Annex 3 should be based on the most recent audited accounts for the relevant entities (or interim accounts where available) updated for any material changes since the Accounting Reference Date provided that such accounts are available in a reasonable timeframe to allow the Supplier to comply with its obligations under this Schedule. If such accounts are not available in that timeframe, to the extent permitted by Law financial information should be based on unpublished unaudited accounts or management accounts (disclosure of which to the Appropriate Authority remains protected by confidentiality).

Schedule 9 - Variation Form

This form is to be used in order to change a Call-Off Contract in accordance with Clause 32 (Variation process)

Contract Details		
This variation is between:	[insert name of Buyer] ("the Buyer") And [insert name of Supplier] ("the Supplier")	
Contract name:	[insert name of contract to be changed] ("the Contract")	
Contract reference number:	[insert contract reference number]	
Details of Proposed Variation		
Variation initiated by:	[delete as applicable: Buyer/Supplier]	
Variation number:	[insert variation number]	
Date variation is raised:	[insert date]	
Proposed variation		
Reason for the variation:	[insert reason]	
A Variation Impact Assessment shall be provided within:	[insert number] days	
Impact of Variation		
Likely impact of the proposed variation:	[Supplier to insert assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: [Buyer to insert original Clauses or Paragraphs to be varied and the changed clause]	
Financial variation:	Original Contract Value:	£ [insert amount]
	Additional cost due to variation:	£ [insert amount]
	New Contract value:	£ [insert amount]

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

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

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

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

Signature _____
Date _____
Name (in Capitals) _____
Address _____

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

Signature _____
Date _____
Name (in Capitals) _____
Address _____

ANNEX A
SOFTWARE AND SPECIFICATION

1 Software Overview

1.1 This Annex, including its Definitions (which only apply in respect of this Annex unless stated otherwise), details the Software and its Modules, Function, capability and Deliverables for the Software Service and Type of Support Service detailed in Table 1 of Schedule 1 to the Agreement.

Table A1: Software

Software	Module (Component) name	Description
Maytas	Maytas Core	Maytas Core will provide users with the following functions: <ul style="list-style-type: none">- Formula funded and non-formula funded contracts- Learner, personnel and organisation records- Bulk updating of records using Global Updater- LRS integration- User permission management- Apprenticeship Service upload- Mail merge- Standard Report Library
	Contact Log	The contact log module allows users to track contact with learners, personnel and organisations. Where used in conjunction with the corresponding Microsoft Outlook plugin emails can be sent from the system and responses tagged against the relevant record.
	ILR Batch	The ILR Batch function will provide users with the ability to generate a batch XML file in line with the ESFA requirements.
	PLR Download	The PLR Download provides the user with direct access to the Learner record Service to see and download personal learning records.
	Reports Generator	The report generator allows users to generate both list and matrix reports from within the

Software	Module (Component) name	Description
		Maytas application. Once reports have been created users can; run, print or export data.
	DAS Upload	The DAS Upload allows users to efficiently send ILR matched data to their DAS accounts directly from Maytas.

ANNEX B – Not used

ANNEX C
SUPPLIER END USER TERMS

1. Supplier End User Terms

1.1 This Annex governs the use of the Supplier Software and the Software Service during the Term.

Definitions	<p>For the purpose of this Annex, the words and expressions below shall have the following meanings:</p> <p>ID: all log-on identifiers, including usernames and passwords, assigned to, or created by the Buyer in order to access or use the Software and/or Software Service;</p> <p>Intellectual Property Rights: patents, utility models, rights to inventions, copyright and related rights, trade marks and service marks, trade names and domain names, rights in get-up, goodwill and the right to sue for passing off or unfair competition, rights in designs, rights in computer software, Database rights, rights to preserve the confidentiality of information (including know-how and trade secrets) and any other intellectual property rights, including all applications for (and rights to apply for and be granted), renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist, now or in the future, in any part of the world;</p> <p>Online Service: computing services and capabilities such as Software, Software Service, software platforms, hardware platforms, infrastructure and similar capabilities, which are delivered by Supplier to the Buyer over a data network (including the Internet), rather than provided locally or on-site. The Software and hardware assets are owned/provided by Supplier and the Buyer is billed for usage;</p> <p>On Premise Software: Software provided in object code form or any other form, which is located on the Buyer's servers or on a third-party provider's servers with whom the Buyer has contracted with the prior written consent of Supplier, as applicable;</p> <p>Open Source Software: open-source software as defined by the Open Source Initiative or the Free Software Foundation;</p> <p>Permitted Purpose: the Buyer's use of the Software and Software Service is restricted to:</p> <div><div>(a)</div><div>the internal business requirements of the Buyer only; and</div></div> <div><div>(b)</div><div>no other use, unless it has the prior written consent of Supplier, which the Buyer acknowledges may be subject to additional Fees if approved by Supplier.</div></div> <p>Permitted Users: the users or groups of users permitted by the Buyer to access and utilise the functionality of the Software and/or Software Service, for example, enrolled students and Learners of the Buyer;</p> <p>Prohibited Content: content that infringes any Intellectual Property Rights or data protection, privacy or other rights of any other person, is defamatory</p>
--------------------	---

	<p>or in breach of any contractual duty or any obligation of confidence, is obscene, sexually explicit, threatening, inciteful of violence or hatred, blasphemous, discriminatory (on any ground), knowingly false or misleading, or that does not comply with all applicable laws and regulations or is otherwise objectionable or prohibited as set out in any acceptable use policy published online through the Software and/or Software Service, as updated by Supplier from time to time;</p> <p>Registered Users: authorised users of the Buyer, for example, stakeholders, enquirers, administrative, teaching or other staff and approved contractors (which specifically excludes any direct or indirect competitor of Supplier) and sponsors of the Buyer who have the ability to access the Software and/or Software Service;</p> <p>Semestry SaaS: the specified Software made available to Registered and Permitted Users as an Online Service;</p> <p>Site: the location agreed by the Parties;</p> <p>Software; the specified software provided by Supplier;</p> <p>Software Service: the applicable service used by the Buyer to access the specified Software, e.g. On Premise Software and/or Tribal Cloud SaaS, Tribal Edge SaaS, and/or Semestry SaaS, and/or Tribal Edge Dynamics SaaS;</p> <p>Tribal Cloud SaaS: the specified Software made available to Registered and Permitted Users as an Online Service;</p> <p>Tribal Edge SaaS; the specified Software made available to Registered and Permitted Users as an Online Service;</p> <p>Tribal Edge Dynamics SaaS: the specified Software made available to Registered and Permitted Users on a third-party provider's servers with whom the Buyer has contracted with the prior written consent of Supplier;</p> <p>Third-Party Software: any software (including Open Source Software) provided by Supplier in connection with the Software Service, and which is integrated into the Software, the copyright of which is not owned by Supplier;</p> <p>Term: the agreed duration for the Software Service.</p>
Intellectual Property Rights	<p>Supplier's Software and the Software Service are protected by copyright and other Intellectual Property Rights. All Intellectual Property Rights (and any other rights) in and to the Software and/or the Software Service are retained by Supplier or its suppliers.</p>
Software Service and Buyer's Rights	<p>In relation to Tribal Cloud SaaS, Tribal Edge SaaS, Semestry SaaS, and Tribal Edge Dynamics SaaS, Supplier grants to the Buyer a non-transferable and non-exclusive right to access and use the Software Service for the Permitted Use for the Term, subject to these End User Terms.</p> <p>In relation to the On Premise Software Service, Supplier grants to the Buyer a non-transferable, non-exclusive, revocable and limited licence to access and use the On Premise Software for the Permitted Use at the Site for the</p>

	Term, subject to these End User Terms.
Use of Software and Service Documentation	Supplier grants to the Buyer a non-transferable, non-exclusive, revocable and limited licence to access and use the applicable Software and Service Documentation and any other materials agreed in writing, for the Permitted Use during the Term.
Buyer Responsibilities	The Buyer shall be responsible for all access to and use of the Software and Software Service by its Registered and Permitted Users. The Buyer shall only provide its Registered and Permitted Users with access to the Software via the Software Service approved by Supplier (e.g. On Premise and/or Tribal Cloud SaaS, Tribal Edge SaaS, and/or Semestry SaaS and/or Tribal Dynamics SaaS). The Buyer shall immediately notify Supplier in the event that the Buyer becomes aware of breach of this obligation by any person.
Buyer to maintain Security and Confidentiality	The Buyer shall be responsible for ensuring the security and confidentiality of all IDs. The Buyer acknowledges and agrees that it will be solely responsible for all activities that occur under such ID. The Buyer shall promptly notify Supplier upon becoming aware of any unauthorised access to or use of the Software and/or Software Service and provide all reasonable assistance to Supplier to bring an end to such unauthorised access or use.
Buyer Obligations	<p>The Buyer shall:</p> <ul style="list-style-type: none"> (a) comply with all applicable laws and regulations with respect to its activities; (b) obtain and maintain all necessary licenses, consents, and permissions necessary for Supplier to perform its obligations, if any; (c) in relation to On Premise Software, keep a complete and accurate record of the Buyer's copying and disclosure of the Software, its location, and its Registered Users, and produce such record to Supplier on request from time to time; (d) pay, for broadening the scope of the licences or metric band to cover use not authorised by Supplier, an amount equal to the Fees which Supplier would have levied had it licensed or granted such unauthorised use on the date when such use commenced together with interest at the rate of 4% above the base lending rate of the reserve bank in the jurisdiction (or if there is no such reserve bank or base lending rate at 4% above the base lending rate of the Bank of England) from such date until the date of payment; (e) in relation to On Premise Software, install it solely and exclusively on designated hardware platforms and only at the Site, not copy the whole or any part of the Software, provided that the Buyer shall be entitled to make one (1) copy of the Software in machine-readable form for back-up purposes only (such copies to be subject to the restrictions relating to use of the On Premise Software). Any change to the Site or any change or replacement to the designated hardware

	<p>platform, by either Party, is to be undertaken by a Change Request Agreement and maybe subject to additional Fees;</p> <p>(f) reproduce on any copy of the Software and/or Software and Service Documentation, any copyright and trademark notice of Supplier and/or any third party proprietor;</p> <p>(g) not, in relation to Tribal Cloud SaaS, install the Software on the Buyer's equipment;</p> <p>(h) not translate, modify, adapt or create derivative works from the Software;</p> <p>(i) not obscure, amend or remove any copyright notice, trademark or other proprietary marking on, or visible during the operation or use of, the Software, Software and Service Documentation or Third-Party Software;</p> <p>(j) not attempt to discover or gain access to the source code for the Software or reverse engineer, modify, decrypt, extract, disassemble or decompile the Software or Third-Party Software (except strictly to the extent that the Buyer is permitted to do so under applicable law in circumstances under which Supplier is not lawfully entitled to restrict or prevent the same), including in order to:</p> <p>(i) build a competitive product or service;</p> <p>(ii) build a product using similar ideas, features, functions or graphics of the Software; or</p> <p>(iii) copy any ideas, features, functions or graphics of the Software;</p> <p>(k) not attempt to interfere with the proper working of the Software and/or Software Service and, in particular, must not endanger its operation, nor attempt to circumvent or endanger security, licence control or other protection mechanisms, or tamper with, hack into or otherwise disrupt the Software and/or Software Service or any associated website, computer system, server, router or any other internet-connected device;</p> <p>(l) not separate the component parts of the Software for use on more than one hosted service without the prior written consent of Supplier</p> <p>(m) not introduce any software virus or other malware that may infect or cause damage to the Software or Software Service;</p> <p>(n) in relation to On Premise Software, not merge or combine the whole or any part of the Software with any other software or documentation, except with the prior written consent of Supplier:</p> <p>(o) not resell, sublicense, rent, lease, sell, assign, lend, transfer, charge, novate or otherwise deal with the Software and/or Software Service and/or this Agreement, or use the Software and/or Software Service, for the benefit of anyone other than the Buyer and not allow or permit a third party to do so;</p> <p>(p) not allow the Software and/or Software Service to become the sub-</p>
--	--

	<p>ject of any charge, lien or encumbrance without the prior written consent of Supplier;</p> <p>(q) not deal in any other manner with any or all of its rights and obligations without the prior written consent of Supplier; and/or</p> <p>(r) not use the Software and/or Software Service:</p> <ul style="list-style-type: none"> (i) to provide any application service provider offering, hosted services or bureau services; (ii) to upload, store, post, email, transmit or otherwise make available any Prohibited Content; (iii) to impersonate any person or entity or otherwise misrepresent the Buyer's relationship with any person or entity; (iv) to engage in any fraudulent activity or further any fraudulent purpose; (v) to provide material support or resources (or to conceal or disguise the nature, location, source, or ownership of material support or resources) to any organisation(s) designated by the government of the applicable jurisdiction or any foreign government as a terrorist organisation; (vi) to "stalk" or otherwise harass another person; (vii) to provide false identity information to gain access to or use the Software and Software Service; (viii) to link or use the Software and Software Service in combination with the software or services of a third party without Supplier's prior written consent and/or without obtaining all necessary permissions and/or licences at no cost to Supplier; (ix) to collect or store personal data about other users in connection with the Prohibited Conduct and activities set out in sub-clauses (r)(i) to (viii); and/or (x) in a manner as prohibited by any third party service provider to Supplier in respect of the Software. Software Service or Services, as advised to the Buyer from time to time, <p>and shall not permit any third party to do any of the foregoing.</p>
Use of Third-Party Software outside scope	<p>The Buyer acknowledges that some of the Software and/or Software Services may include Third-Party Software. Any use of Third-Party Software is subject to the rights and obligations under such third-party's licence. To the extent there is a conflict between this Schedule and the third-party licence, the terms of the applicable third-party licence shall control (in respect of the Third-Party Software). These End User Terms apply to any Third Party Software provided with the Software and/or Software Service.</p>
Export	<p>Neither party shall export, directly or indirectly, any technical data acquired from the other party (or any products, including software, incorporating any such data) in breach of any applicable laws or regulations, including United</p>

	States export laws and regulations, to any country for which any government (or any agency thereof), at the time of export, requires an export licence or other governmental approval without first obtaining such licence or approval.
Termination	Without prejudice to any other rights, Supplier may terminate or suspend the Buyer's rights to access and use the Software and Software Service if the Buyer fails to comply with these terms in any material respect. In the event of termination or suspension the Buyer must stop using and/or accessing the Software and Software Service.

ANNEX D.1

CORE SUPPORT SERVICES

1. Core Support Service Description

Scope	This Annex including Definitions, describes the Core Support Services to be performed by The Supplier, in respect of the Software and Software Service during the Term. This Annex is to be read in conjunction with other Annexures detailed in Types of Support Services (detailed in the Definitions (if any)) and the order of precedence will be as set out in Annex D.1 to D.6 (as applicable).
Supersede Other Agreements	This Annex is intended to supersede and replace all other previous agreements between Supplier and the Buyer, in relation to Support Services, including those detailed in an Agreement, if any.
Inconsistency	To the extent of inconsistency between the terms of this Annex and the terms of the Call-Off Contract, the terms of this Annex shall prevail.
Not Interfere with Customer Operations	Supplier will use Commercially Reasonable Efforts to co-ordinate the provision of Support Services with the Buyer so as not to interfere with the operations of the Buyer.
Support Requests	<p>In order for Supplier to be able to provide Support Services to the Buyer, it will be necessary (and is a condition of this Agreement) for the Buyer to:</p> <ul style="list-style-type: none"> (a) submit a Request to Supplier through the Customer Portal which includes, a detailed description of any Fault requiring Support Services, including where possible a screenshot, and the circumstances in which it arose, upon becoming aware of the Fault. The Buyer shall provide such additional information and access as may be reasonably requested by Supplier to enable the Fault to be classified; (b) maintain the Software such that the current version is Supported Software except where Supplier is in breach of this Agreement; (c) for On-Premise Software and Tribal Edge Dynamics SaaS, ensure that appropriate arrangements are put into place to allow remote access to the system by modem, internet or some other appropriate arrangement in accordance with Buyer remote access security policies and which are acceptable to Supplier; and (d) continue to maintain any system requirement in accordance with the minimum operating requirements as notified by Supplier or the owner thereof from time to time with reasonable notice.
Designated Customer Support Staff	It is critical to the productive and efficient provision of Supplier's Support Services that it is not used as an unofficial training service for the Software and/or Software Service. Accordingly, Supplier requires that only the Buyer's Designated Customer Support Staff access the Support Services in relation to the Software and/or Software Services, failing which Supplier shall not be required to provide Support Services.
Tribal Global Service Desk	The Parties acknowledge and agree that Supplier may transfer Personal Data to Supplier Affiliates for the purposes of providing Services, including Support Services. In respect of such transfers, Supplier warrants that it shall only transfer Personal Data to Supplier Affiliates under an adequate data transfer mechanism in accordance with Data Protection Legislation, including to Supplier Affiliates who

TRIBAL

	have entered into the Tribal Intra-Group Personal Data Transfer Agreement. Supplier warrants that such Tribal Intra-Group Personal Data Transfer Agreement provides an adequate level of protection of the privacy and fundamental rights and freedoms of individuals as required by applicable Data Protection Legislation.
On-Site Support Services	Except as specifically provided, on-site support is outside the scope of Support Services and will only be delivered by way of an agreed Change Request.
Advance Notice of Material Changes	The Buyer acknowledges that Supplier may from time-to-time Update/Upgrade the Software and/or Software Service which may result in changes to the appearance and/or functionality of the Software and/or Software Service, provided that the Software and/or Software Service will continue to conform with the Supplier Warranties and remain materially suitable for the business purpose for which it was purchased. Supplier shall take reasonable steps to advise the Buyer, in advance, of any material changes that will occur in respect of the appearance and/or functionality of the Software and/or Software Service.
Unsupported Software	Without prejudice to the terms of this Agreement, in the event that the Buyer's Production Environment is Unsupported Software, Supplier's obligation to provide Support Services will cease and a warranty-free right to use shall come into immediate effect for the Unsupported Period but no longer than the Term. Notwithstanding any Unsupported Period, the Buyer's obligation to pay Support Service Fees (including as part of Annual Subscription Fees) will continue in accordance with the terms of this Agreement. This clause will cease to apply so long as the Buyer's Production Environment is Supported Software and all Fees have been paid. This clause is subject to the provisions in Tribal SaaS and Tribal Cloud SaaS Annexures. This clause will not apply in the event that the Buyer's inability to be on Supported Software is due to Supplier's failure to comply with its obligations under the Agreement.

2. Key Details of Core Support Services

Commencement Date	Effective Date unless otherwise agreed between the Parties in writing.
Supported Software	The Software detailed in Table 1 of Schedule 1 to the Agreement, where the Type of Support Service is Core Support Services.
Support Hours / Support Days	The Working Hours / Working Days as set out in section 4 (Definitions) of Annex D.1 when the Core Support Services will be provided (" Support Hours ").
Access to Core Support Services	<p>Core Support Services are accessed via Supplier's Service Desk using Self Service Tools.</p> <p>The Self Service Tools comprise:</p> <ul style="list-style-type: none"> Customer Portal: a web-based tool for reporting Incidents available 24 hour by 365-day basis (excluding scheduled down time). Tribal Communities: a web-based searchable knowledge base, providing access to Frequently Asked Questions (FAQs), Wiki pages and a list of previously reported issues that have been identified within the versions of the Software.

TRIBAL

Levels of Core Support Services	<p>Supplier delivers its Core Support Services via three-levels:</p> <ul style="list-style-type: none"> • Level 1 Support; • Level 2 Support; and • Level 3 Support, <p>in accordance with the Service Level Targets in clause 3.</p>
Level 1 Support	<p>The Service Desk is staffed to provide a single point of contact for Designated Customer Support Staff to report (through the Customer Portal) and progress Incidents relating to the use of the Software and Software Service.</p> <p>Where an Incident is not raised through the self-service portal form, the Level 1 Support team will document each Incident into the Customer Portal and will issue a case number to the Buyer.</p> <p>The Level 1 Support Team (Service Desk) will undertake initial analysis of an Incident and undertake basic triage to attempt to identify the root cause.</p> <p>If the Incident cannot be resolved at Level 1 then it will be escalated to Level 2 Support. This may be necessary where a greater depth of technical knowledge or where specialist skills or capability is required to resolve the incident.</p>
Level 2 Support	<p>Level 2 Support will undertake deeper and more specialised investigation of an Incident in an attempt to identify the root cause and rectify the Incident.</p> <p>Where an Incident is identified that cannot be reproduced, Level 2 Support will typically contact the Buyer to obtain more information in order to reproduce the Fault. Where a Fault does not re-occur and cannot be reproduced by Supplier then it will be necessary to close the Incident.</p> <p>Escalation to Level 3 Support may be required where a problem is highly complex or requires changes to the underlying Application code or Infrastructure.</p>
Level 3 Support	<p>Level 3 Support is the highest level of technical expertise which may involve Updates or other corrective actions.</p>
Support Service Procedure	<p>In relation to the Service Level Targets:</p> <ul style="list-style-type: none"> • the periods of time for the provision of a Resolution shall commence at the time the Buyer has logged the request with the Service Desk through the Customer Portal. The time calculated to provide a Resolution shall exclude any time when Supplier is: <ul style="list-style-type: none"> ○ waiting on a response from the Buyer; ○ deployment of a Resolution is delayed due to the action or in-action of the Buyer; or ○ where it has not been possible to replicate an issue and the issue has not re-occurred; • where Supplier has provided instructions for a Work Around for the Fault, the Buyer shall apply/follow it as soon as reasonably practicable. A Work Around may be deemed to be the final corrective action depending on the Priority of the Fault; • in the event that Supplier cannot identify a Work Around for the Fault or provide a Resolution within the relevant Resolution SLT it shall notify the Buyer of the date by which it reasonably believes it shall provide a Work Around or Resolution and shall use Commercially Reasonable Efforts to

TRIBAL

	<p>meet this date;</p> <ul style="list-style-type: none">the objective description of the Fault and/or Priority will be used to determine the actual Priority level. The Buyer will typically report an Incident and set an initial Priority designation. Supplier will commence triage in respect to the Buyer's Priority designation and subject to findings will determine the Priority designation. Any changes (increases or decreases) in Priority level will be communicated to the Buyer by Supplier;where Fault and/or Priority designation is changed, the time to provide a Resolution will change to the corresponding Priority level values and SLT. For example, if a Fault designation is to be increased the SLT will be shortened; where a Fault designation is decreased, the SLT will be lengthened;where a reasonable and effective Work Around is provided against a Priority 1 or 2 fault designation, the Resolution SLT will be changed to the Priority 3 SLT or lower as appropriate; andin the event that the Buyer disagrees with the designation set by Supplier, it shall be entitled to escalate the designation in accordance with the Support Services Escalation Procedure.																
Support Services Escalation Procedure	<p>Where a Fault, Restoration Request or Alert is not Resolved in accordance with the SLTs, or there is a material unresolved issue in relation to a designated Fault Type, the Buyer shall be entitled to escalate the matter in accordance with the following table:</p> <p>Table D.1:1: Core Support Services Escalation Levels</p> <table><tr><th>Escalation Level</th><th>Contract Person</th><th>Email</th><th>Timeframe</th></tr><tr><td>1</td><td>Support Service Desk Manager</td><td>Support.desk.manager@tribalgroupp.com</td><td>Within 1 Support Hour of the Fault level being designated by Supplier</td></tr><tr><td>2</td><td>Regional Customer Services Manager</td><td>EMEA - customer.services.manager.emea@tribalgroupp.com APAC - customer.services.manager.apac@tribalgroupp.com</td><td>Within 2 Support Hours of the Fault level being designated by Supplier</td></tr><tr><td>3</td><td>Global Service Delivery Director</td><td>service.delivery.director@tribalgroupp.com</td><td>Within 7 Support Hours of the Fault level being designated by Supplier</td></tr></table> <p>Supplier shall upon request from the Buyer notify the Buyer of the identity of the individuals holding each of the above positions.</p> <p>Notwithstanding the Buyer exercising its right to escalate the dispute, Supplier shall continue to work towards the provision of a Work Around or Resolution of such Fault.</p>	Escalation Level	Contract Person	Email	Timeframe	1	Support Service Desk Manager	Support.desk.manager@tribalgroupp.com	Within 1 Support Hour of the Fault level being designated by Supplier	2	Regional Customer Services Manager	EMEA - customer.services.manager.emea@tribalgroupp.com APAC - customer.services.manager.apac@tribalgroupp.com	Within 2 Support Hours of the Fault level being designated by Supplier	3	Global Service Delivery Director	service.delivery.director@tribalgroupp.com	Within 7 Support Hours of the Fault level being designated by Supplier
Escalation Level	Contract Person	Email	Timeframe														
1	Support Service Desk Manager	Support.desk.manager@tribalgroupp.com	Within 1 Support Hour of the Fault level being designated by Supplier														
2	Regional Customer Services Manager	EMEA - customer.services.manager.emea@tribalgroupp.com APAC - customer.services.manager.apac@tribalgroupp.com	Within 2 Support Hours of the Fault level being designated by Supplier														
3	Global Service Delivery Director	service.delivery.director@tribalgroupp.com	Within 7 Support Hours of the Fault level being designated by Supplier														

TRIBAL

Service Engagement and Reporting	<p>Service Engagement and Reporting covers communication during the Resolution of Critical and Major Faults in the Supported Environments only and the provision of Reports following the Resolution of these Incidents. Wherever possible a Report will be provided more quickly than the times given below.</p> <p>Service reporting includes:</p> <ul style="list-style-type: none">• Critical Fault Report;• Major Fault Report; and• Root Cause Report. <p>Depending on the nature of the Fault and the time needed to determine the root cause, the Root Cause Report may be combined with the Critical Fault Report or the Major Fault Report.</p>								
	<p>Table D.1:2: Core Support Services - Critical Fault (Priority 1) communications and engagement</p> <table><tr><th>Report Timeframe</th><th>Report</th></tr><tr><td>After initial triage and diagnosis</td><td>If Resolution is clear and straightforward, then this will be actioned. If not, a Major Incident Team will be assembled and a MI Manager will be appointed. The Buyer will be provided with the MI Manager name and contact details.</td></tr><tr><td>Within 1 Support Hour</td><td><p>In addition to basic data such as case number, date and time, Buyer contact details and Software version details, the parties will seek to provide the following information via Customer Portal:</p><ul style="list-style-type: none">• a problem statement;• a business impact assessment;• a description of the symptoms experienced;• any steps identified to reproduce the problem;• reference to evidence such as log files or screen shots to support reasoning; and• reference to any significant changes that have been carried out prior to the incident occurring.<p>Customer Portal updates will continue to be provided in real time and automatically notified to the Buyer by email.</p><p>Further updates will be provided on an on-going basis, typically via email or a telephone call.</p></td></tr><tr><td>Critical Incident Management</td><td>A Critical Fault Incident Bridge will be opened using Microsoft Teams or other suitable technology. The Incident Bridge will allow for continuous monitoring of the technical plan and</td></tr></table>	Report Timeframe	Report	After initial triage and diagnosis	If Resolution is clear and straightforward, then this will be actioned. If not, a Major Incident Team will be assembled and a MI Manager will be appointed. The Buyer will be provided with the MI Manager name and contact details.	Within 1 Support Hour	<p>In addition to basic data such as case number, date and time, Buyer contact details and Software version details, the parties will seek to provide the following information via Customer Portal:</p> <ul style="list-style-type: none">• a problem statement;• a business impact assessment;• a description of the symptoms experienced;• any steps identified to reproduce the problem;• reference to evidence such as log files or screen shots to support reasoning; and• reference to any significant changes that have been carried out prior to the incident occurring. <p>Customer Portal updates will continue to be provided in real time and automatically notified to the Buyer by email.</p> <p>Further updates will be provided on an on-going basis, typically via email or a telephone call.</p>	Critical Incident Management	A Critical Fault Incident Bridge will be opened using Microsoft Teams or other suitable technology. The Incident Bridge will allow for continuous monitoring of the technical plan and
Report Timeframe	Report								
After initial triage and diagnosis	If Resolution is clear and straightforward, then this will be actioned. If not, a Major Incident Team will be assembled and a MI Manager will be appointed. The Buyer will be provided with the MI Manager name and contact details.								
Within 1 Support Hour	<p>In addition to basic data such as case number, date and time, Buyer contact details and Software version details, the parties will seek to provide the following information via Customer Portal:</p> <ul style="list-style-type: none">• a problem statement;• a business impact assessment;• a description of the symptoms experienced;• any steps identified to reproduce the problem;• reference to evidence such as log files or screen shots to support reasoning; and• reference to any significant changes that have been carried out prior to the incident occurring. <p>Customer Portal updates will continue to be provided in real time and automatically notified to the Buyer by email.</p> <p>Further updates will be provided on an on-going basis, typically via email or a telephone call.</p>								
Critical Incident Management	A Critical Fault Incident Bridge will be opened using Microsoft Teams or other suitable technology. The Incident Bridge will allow for continuous monitoring of the technical plan and								

T R I B A L

		<p>Buyer staff will be added to the Incident Bridge as required.</p> <p>In addition to the basic information communicated via the Customer Portal, a technical plan of action will be communicated. This will typically include:</p> <ul style="list-style-type: none"> technical steps to Resolve Incident or provide a Work Around; contingencies if steps do not Resolve the Incident; timeframes for each step; an indication of the expected duration of any downtime or loss of service; and Buyer approvals and/or actions required to undertake recovery. <p>Additional steps and plans will be discussed and communicated until the fault has been Resolved or a Work Around provided.</p>
	Further escalation as required	The incident will be escalated internally within Supplier as required including to product development and other teams necessary to investigate and remediate the Incident.
	Within 4 Support Days, a Root Cause Report will be provided	A Root Cause Report will be provided to the extent that the necessary information is available.
Table D.1:3: Core Support Services - Major Fault (Priority 2) communications and engagement		
	Report Timeframe	Report
	After initial triage and diagnosis	If Resolution is clear and straightforward, then this will be actioned. If not, then an Incident manager will be assigned and they will manage the Incident through to resolution.
	Within 2 Support Hours	<p>In addition to basic data such as case number, date and time, Buyer contact details and Software version details, the parties will seek to provide the following information via the Customer Portal:</p> <ul style="list-style-type: none"> a problem statement; a business impact assessment; a description of the symptoms experienced; any steps identified to reproduce the problem; and reference to any significant changes that have been carried out prior to the

TRIBAL

		<p>incident occurring.</p> <p>Customer Portal updates will continue to be provided in real time and automatically notified to the Buyer by email.</p>
	Major fault management	<p>An Incident Bridge may be opened as required using Microsoft Teams or other suitable technology. The Incident Bridge will allow for continuous monitoring of the technical plan and Buyer staff will be added to the Incident Bridge as required.</p> <p>In addition to the basic information communicated via the Customer Portal, a technical plan of action will be communicated. This will typically include:</p> <ul style="list-style-type: none"> • technical steps to Resolve Incident or provide a Work Around; • contingencies if steps do not Resolve the Incident; • timeframes for each step; • an indication of the expected duration of any downtime or loss of service; and • Buyer approvals and/or actions required to undertake recovery. <p>Additional steps and plans will be discussed and communicated until the fault has been Resolved or a Work Around provided.</p>
	Further escalation as required	The incident will be escalated internally within Supplier as required including to product development and other teams necessary to investigate and remediate the issue.
	Within 7 Support Days a Root Cause Report will be provided	The Root Cause Report will be provided to the extent that the necessary information is available.
Excluded Support Services	<p>The following events are Excluded Support Services and are not included in Core Support Services:</p> <ul style="list-style-type: none"> • misuse or incorrect use of the Software and/or Software Services, use of the Services in combination with equipment or software not designated by Supplier for use with the Services or otherwise contrary to the terms of this Agreement; • operator error; • the use of the Software and /or Software Services for a purpose either for which it has not been designed or which was not specified by the Buyer in writing to Supplier prior to delivery of the Software and/or Software Services to the Buyer; • the use of the Software and/or Software Services on inappropriate equipment; 	

TRIBAL

	<ul style="list-style-type: none"> Incidents arising from any Business Configuration; the failure by the Buyer to implement recommendations in respect of or solutions to Fault, previously advised by Supplier; the failure of any hardware including the Operating System for the hardware, save where such Infrastructure is provided in accordance with this Agreement; the Buyer's failure to maintain and manage hardware in accordance with the hardware supplier's recommendations, including the application of firmware Updates and security patches, save where such Infrastructure is provided in accordance with this Agreement; where a Third-Party Proprietor provided software or infrastructure upon which the Software and/or Software Services are dependent (but which is not included in the Services), ceases to support such software; examples include, but may not be limited to Operating System, internet browsers, Database versions; the provision of any security compliance requirements over those specified in this Schedule; where the need for Support Services arises from the Buyer's failure to abide by the General Terms of this Agreement; any configuration of the Software and/or Software Service or Customer Data that is not consistent with the typical use of the Software and/or Software Service unless otherwise agreed in writing by the Parties; if malfunctions or defects are due to improper use of the Software and/or Software Service, or for any reason external to the Software and/or Software Services, including, but not limited to, failure or fluctuation of electrical supplies, hardware failures, accidents or natural disasters; advice on problems experienced by the Buyer in operating the Software which do not fall within the scope of the Core Support Services; consultation regarding enhancement of the Software; and training in the use and/or operation of the Software and/or Software Service. Supplier may, upon request by the Buyer, provide Additional Services to assist in the resolution of Excluded Support via a written agreement between the Parties.
Customer Responsibilities	<p>Customer Responsibilities include:</p> <ul style="list-style-type: none"> providing suitable user access devices; prompt notification of any Software malfunction; and providing Supplier with access to staff in a timely manner to Resolve any Incident, where the root cause is unclear.

3. Service Level Targets for Core Support Services

Response and Resolution	Supplier shall use Commercially Reasonable Efforts to achieve the stated Service Level Targets ("SLT") in respect of the Responses ("Response SLT") and Resolutions ("Resolution SLT"). Wherever possible, a Response or Resolution
--------------------------------	---

TRIBAL

will be provided more quickly although the times indicated are targets. For clarity, SLTs only apply within the Support Hours.

The following table details the SLTs for the Production Environment:

Table D.1:4: Core Support Services - Service Level Targets

Fault Type	Response SLT	Resolution SLT	Typical Resolution Objectives
Critical Fault (Priority 1)	30 minutes during a Support Day	8 Support Hours	To provide a Fault correction or reasonable Work Around. Resolution may involve a re-starting of the Software or Software Service, alterations to the configuration of the Production Environment, a restore from a previous version, or the application of a fix to a previously reported issue.
Major Fault (Priority 2)	1 Support Hour	3 Support Days	To provide a Fault correction or reasonable Work Around. Resolution may involve a re-starting of the Software or Software Service, or a restore from a previous version, or the application of a fix to a previously reported issue.
Important Fault (Priority 3)	4 Support Hours	20 Support Days	This Priority level has a Work Around available.
Minor Fault (Priority 4)	8 Support Hours	No SLT Commitment	This Priority level has a Work Around available and may involve the issue of an Update.

Unless specified otherwise in this Agreement, where a Fault is reported outside the Support Hours the Response SLT and Resolution SLT start times (for the purpose of calculating Response and Resolution targets) will begin from the start of the next Support Hours period.

TRIBAL

2. Definitions

The Definitions applicable to this Annex are detailed below. The Definitions also include defined terms that are used in the following further Supplier Annexures, which may be applicable:

- Annex D.2 – Tribal Software Support Services;
- Annex D.3 – Tribal Cloud SaaS;
- Annex D.4 – Tribal Edge SaaS;
- Annex D.5 – Tribal Dynamics SaaS; and
- Annex D.6 – Semestry SaaS.

Definitions

- **AFD Address Lookup Solution:** address verification services that customers with the designated Components, and a valid AFD service subscription can access from within the Software Service to verify addresses;
- **Affiliates:** in relation to a Party, any other entity which directly or indirectly Controls is Controlled by, or is under direct or indirect common Control with that Party from time to time;
- **Agreement:** the Call-Off Contract entered into between Supplier and the Buyer for the provision of the Software and which annexes this Annex;
- **Alerts:** a system generated response to a pre-determined condition that outlines whether the condition exceeds a limit and is used for the purpose of monitoring and shall be categorised using the SLTs in Annex D.1;
- **Application:** means the Software;
- **Application Management Services:** as set out in Annex D.3, as applicable;
- **Availability or Available:** the extent to which an Application is operational, functional and usable for completing or fulfilling a Buyer's business requirements for which the Software Services were purchased and determined in accordance with Annex D.3 and Annex D.4, as may be applicable to the Software Service;
- **Backup:** the copying of data to alternative media for the purposes of future recovery should this be needed;
- **Backup and Restore:** as set out in Annex D.3 and Annex D.4, as applicable;
- **Bot:** software that is designed to automate interaction and use of Software and/or Software Services;
- **Bulk Data Interface:** a type of system to system interaction that involves the transfer of larger quantities of data, typically more than can be accommodated by an API;
- **Business Configuration:** configuration and customisation of the Software to meet the business requirements of the Buyer, and in relation to the following Software, it includes but is not limited to:
 - (i) Blueprints – configuration of workflow / tasking, reports, reference data setup, business process definitions, business rules set up
 - (ii) ebs – ebs client screen configuration (SMC), ontrack staff and learner hub page configuration (Designer), custom web service endpoints (Designer), BI Dashboard configurations (ebs Intel), workflow, reference data setup, data miner views, SSRS reports and the creation and configuration of any archiving routines;
 - (iii) Engage - defining configuration through the Configuration Editor, defining roles through the Role Editor including user permissions, maintenance of

TRIBAL

branding material, the Apple Developer Account Enrolment and any Business Configuration necessary in the source student management system (SITS:Vision, ebs, Maytas/e-track or Tribal Edge Dynamics) and related activities;

- (iv) K2 - grid layouts, custom grid filters, workflows, attribute manager setup, reference data setup, SSRS reports and K2 Portal colour schemes, logos and custom content;
 - (v) Maytas and e-track - screen configuration and design (Maytas Screen Design), e-track screen configuration and design (e-track Screen Design), online application configuration (Online Applications), process design (Process Design Module), BI Dashboard configuration (Business Intelligence), reference data setup, SSRS reports, list reports (Report Generator), digital authentication and the creation and configuration of any archiving routines;
 - (vi) Semestry - TermTime – configuration of database parameters, adjustment of object types, reference data set up, language pack;
 - (vii) Semestry - My Timetable – interface configuration, content of timetable reports, messaging templates;
 - (viii) SID - those configuration options that are made available via SID's system administration screen;
 - (ix) SITS:Vision – creation and configuration of TUPS, Vistas, workflow/tasking, reports, SRL, reference data setup, business process definitions, business rule set up, e:Vision configuration and any archiving routines;
 - (x) Tribal Dynamics – form layout, labels, workflows, business process flows, business rules, views, charts, dashboards, apps (model / canvas / power), security roles, teams, queues, business units, portal content and layout, email templates, business data (such as languages, countries, nationalities, enquiry types, enquiry routing, academic years, disability types courses etc), and the creation and configuration of any archiving routines.
- **BAU or Business as Usual:** the Software and/or Software Service operating in a Production Environment;
 - **Capacity Management:** as set out in Annex D.3;
 - **Change Management:** as set out in Annex D.3 and Annex D.4, as applicable;
 - **Change Request:** a note which details the impact a proposed change will have on any part of this Agreement and signed by Supplier and the Buyer;
 - **Cloud Provider:** a third party contracted by Supplier to provide the underlying infrastructure and services used by the Tribal Edge SaaS and Tribal Cloud SaaS;
 - **Cloud Region:** in relation to Tribal Edge SaaS and Tribal Cloud SaaS, the physical location(s) by country or region of Supplier's Cloud Provider where the computing hardware and software used to store, host and process the Customer Data in the Supported Environments and as detailed in the respective Annexures;
 - **Cloud Service Health and Performance Report:** a report detailing the following information:
 - (i) Application Availability;
 - (ii) System Performance Measures;
 - (iii) Database Resource;
 - (iv) Consumption Metrics;
 - (v) Incident Statistics; and

TRIBAL

- (vi) Service Requests raised within the previous month.
- **Cloud Types:** either:
 - (i) Shared Cloud: Dedicated Environments for each Buyer, excluding the Infrastructure which is shared with a number of customers; or
 - (ii) Dedicated Cloud: Dedicated Environments for the Buyer; or
 - (iii) Multi-tenanted: Multiple customers operating within a single Application instance and infrastructure simultaneously;
- **Commercially Reasonable Efforts:** the same degree of priority and diligence with which Supplier meets the needs of its other similar customers as would be expected by an experienced software supplier of similar size and resources;
- **Continuous Service Improvement:** as set out in Annex D.3 and Annex D.4, as applicable;
- **Critical Fault (Priority 1 or P1):** a Fault where the Production Environment becomes totally non-operational, or the Fault prevents the Buyer materially operating the business for which the Software and/or Software Service was purchased; or any Fault that puts any legal or statutory requirement at imminent risk or a Fault where the Production Environment is down. Access to the Software Service from the public internet (in relation to Tribal SaaS and Cloud Services) ceases to operate due to a Software and Software Service failure and prevents the Buyer operating the business for which the Software and Software Service purchased;
- **Critical Fault Report:** a Report that reviews the Critical Fault and outlines in-depth steps carried out to Resolve the Critical Fault;
- **Cron:** time-based job scheduler;
- **Customer:** the Buyer as defined in the Agreement, and does not extend to any Affiliates of the Buyer unless expressly agreed between the Parties in writing. Nor does it extend to any foreign entities, branches or offices based abroad of the same name and/or company number;
- **Customer Business Continuity Event:** an event that prevents the Buyer from operating the Software from the Buyer's environment;
- **Customer Data:** all information inputted, uploaded and entered via the Online Service by or on behalf of the Buyer, its Registered Users or its Permitted Users;
- **Customer Portal:** tool to allow the Buyer to log Faults and support requests with Supplier;
- **Customer Responsibilities:** as set out in Annex D.1, Annex D.3 and Annex D.4, as applicable;
- **Customer Success Manager:** as set out in Annex D.3, as applicable;
- **Customised Code:** Buyer specific coding that has been created to deliver the Buyer solution and is outside the standard product code;
- **Database:** a repository within a computer that contains structured data and which can be interrogated and updated using a query language, typically SQL (Structured Query Language). A Database is used to store the structured data for Applications such as SITS, ebs and Engage;
- **Design Review:** a review against the standards agreed by the Interface Design Authority for interfaces into the Supported Software;
- **Designated Customer Support Staff:** the staff nominated by the Buyer to receive the Support Services who have been trained to a reasonable level of knowledge and competence in relation to the Software and/or Software Services;

TRIBAL

- **Designated Supplier Personnel:** Supplier Personnel who proactively monitor KPIs for impact on Availability and as set out in Annex D.3, if applicable;
- **Disaster Event:** a typically rare event that materially prevents normal operations from continuing for an extended period. For instance, the loss of Internet connectivity or the loss of one or more datacentres from which a computer service is delivered;
- **Disaster Recovery:** as set out in Annex D.3 and Annex D.4, as applicable;
- **Disaster Recovery Event:** means a disaster or disruption event that disrupts, or is likely to disrupt, the ability of the Buyer to receive the Services or the ability of Supplier to provide the Services and of a scale normally considered within the Buyer's own plans and tests where the cause does not prevent the recovery of the service within the Cloud Regions from which the Services normally operate;
- **Disaster Recovery Plan or DRP:** the disaster recovery and business continuity plan agreed by Supplier and the Buyer which will detail the scenarios for Disaster Events and the actions required to restore the Tribal Edge SaaS and Tribal Cloud SaaS. The DRP will (i) include the Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO), (ii) roles and responsibilities of Supplier and the Buyer, and (iii) the agreed frequency of testing, which will be no more frequent than once every 12 months;
- **Downstream Systems:** Buyer managed systems that take data from the Tribal SaaS and Cloud Services;
- **ebs:Cloud:** ebs delivered to the Buyer via the Tribal Cloud SaaS together with the Support Services;
- **ebs Single Sign On Solution:** the ability to use an external identity provider to authenticate users of the ebs Central application through the remote application delivery capability within the ebs:Cloud Service;
- **Effective Date:** the date set out in an Agreement;
- **Engagement Services:** as set out in Annex D.3, if applicable;
- **Environment Monitoring:** as set out in Annex D.3 and Annex D.4, as applicable;
- **Environment/s:** are a combination of the Software, Software Service, any Third-Party Software, the Platform and Infrastructure required to operate the Software and/or Software Service and as detailed in Annex D.3 and Annex D.4, as applicable. For Tribal SaaS and Cloud Services, the Environments are managed and controlled by Supplier and the demarcation point separating the Environment from any other infrastructure is the ingress point from the Internet;
- **Escalation Procedure:** as set out in Annex D.1;
- **Excluded Support Services:** as set out in Annex D.1, Annex D.2, Annex D.3 and Annex D.4, as applicable;
- **Extended Archive Retention:** as set out in Annex D.3, if applicable;
- **Extended Disaster Event:** means a disaster or disruption event that disrupts, or is likely to disrupt, the ability of the Buyer to receive the Services or of the ability of Supplier to provide the Services where the cause prevents the recovery of the services within the Data Regions from which the Services normally operate;
- **Fault:** A defect in the Software and/or Software Service which is categorised by severity as one of Critical Fault, Major Fault, Important Fault or Minor Fault;
- **Go Live:** when Software and/or Software Service is provided to a Buyer in a Production Environment as part of the Software Service and in which the Buyer processes production business transactions;

TRIBAL

- **Go Live Date:** the date upon which Go Live is achieved;
- **Gradintelligence Cloud Service:** the connector between the SITS Application in SITS:Cloud and the Gradintelligence cloud service;
- **Important Fault (Priority 3 or P3):** a Fault in the Environment that is important, which does not constitute a Critical Fault nor a Major Fault or where the Environment is not functioning normally but the Incident does not constitute a Critical or Major Fault; or any other non-immediate task; or where the Environment is functioning within acceptable parameters, but assistance is required or where there is a Service Desk type question;
- **Incident:** actual or perceived non-compliant behaviour of the Software and/or Software Service. This may be due to a Fault, data quality, misconfiguration by the Buyer, errors by the operator or another cause;
- **Incident Bridge:** escalated support wherein a number of Supplier resources are assigned to facilitate cross discipline sharing to expedite Incident Resolution and to which Buyer staff may participate;
- **Incident Management and Problem Management:** as set out in Annex D.3;
- **Incident Response and Resolution:** as detailed in Annex D.3, Clause 4, and/or Annex D.4, as applicable;
- **Incident Statistics:** Data showing the numbers of Incidents raised and resolved by Incident category within a Service Period. For each P1 and P2 Incident, detailed data on the nature of the Incident and the Resolution of the Incident;
- **Infrastructure:** the combination of computer, storage and network resources, both physical and logical, and the associated software to operate the Infrastructure;
- **Infrastructure Management:** as set out in Annex D.3;
- **Infrastructure Services:** as set out in Annex D.3;
- **Initial Term:** as defined in the Agreement;
- **Intellectual Property Rights:** patents, utility models, rights to inventions, copyright and related rights, trade marks and service marks, trade names and domain names, rights in get-up, goodwill and the right to sue for passing off or unfair competition, rights in designs, rights in computer software, Database rights, rights to preserve the confidentiality of information (including know-how and trade secrets) and any other intellectual property rights, including all applications for (and rights to apply for and be granted), renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist, now or in the future, in any part of the world;
- **Interface:** a system to system data exchange that involves one data flow between the two systems. The Interface can be used to exchange data or to initiate an action of some form. The Interface can be implemented using a range of technologies including but not exclusively, flat file transfer, API interaction and publish/subscribe/event driven technologies;
- **Interface Design Authority:** a group of relevant stakeholders from each of the Parties who meet to collaborate and agree the architecture strategy for the Software and Software Services including the interfacing strategy and standards with the aim of moving the Supported Software architecture closer to leading practice and industry standards;
- **Jurisdiction:** as set out in the Agreement;
- **Level 1 Support:** as set out in Annex D.1;
- **Level 2 Support:** as set out in Annex D.1;

TRIBAL

- **Level 3 Support:** as set out in Annex D.1;
- **Maintenance Window:** either a Scheduled Maintenance Window or Unscheduled Maintenance Window;
- **Major Fault (Priority 2 or P2):** a Fault when the Production Environment experiences a loss of significant functionality, which does not constitute a Critical Fault; or the Fault significantly interferes with a material part of the business for which the Buyer purchased the Software and Software Service or where the Production Environment is accessible but in a reduced state (e.g. time outs or slow response);
- **Major Fault Report:** a Report that reviews the Major Fault and outlines in-depth the steps carried out to Resolve the Major Fault;
- **Major Incident Team:** a team of relevant Supplier Personnel appointed to triage, diagnose, Resolve and provide Reports in relation to a Critical Fault (Priority 1);
- **Major Release:** any improved, modified or corrected version of any Software from time to time issued by Supplier that is deemed by Supplier to be a new version of the Software;
- **Maytas:Cloud:** Maytas delivered to the Buyer via the Tribal Cloud SaaS together with the Support Services, as detailed in this Agreement;
- **MI Manager:** a manager of a Major Incident Team;
- **Minor Fault (Priority 4 or P4):** a Fault in the Environment, which does not constitute a Critical Fault, a Major Fault or an Important Fault;
- **Minor Release:** any improved, modified or corrected version of any Software intended to address Incidents;
- **Modification:** any and all changes, configurations (including Business Configuration), improvements, enhancements and derivative works to the Supplier IPR;
- **Module or Component:** any part of the Software identified separately;
- **Non-Production Environment:** the Environment in which the Buyer performs transactions against non-production data, examples of which include environments for training, interface testing, and quality testing, as required;
- **On Site:** a physical location occupied or controlled by the Buyer or such other location that the Buyer may request Supplier to attend to provide the Services;
- **Online Service:** computing services and capabilities such as Software, Software Service, software platforms, hardware platforms, infrastructure and similar capabilities, which are delivered by Supplier to the Buyer over a data network (including the Internet), rather than provided locally or on-site. The Software and hardware assets are owned/provided by Supplier and the Buyer is billed for usage;
- **Open Source Software:** open-source software as defined by the Open Source Initiative or the Free Software Foundation;
- **Operating Systems:** the software provided to operate physical or logical components of the Infrastructure;
- **Operational Time or OT:** the total number of minutes in a Service Period (excluding any regular Scheduled Maintenance Windows and any other Scheduled Maintenance Windows for Upgrades agreed with the Buyer);
- **Other Systems:** means Systems other than the Software or Software Services to which the Software or Software Service is linked via an Interface;
- **PanIntelligence Reporting Solution:** a reporting solution provided by PanIntelligence and delivered by Tribal Cloud SaaS;

TRIBAL

- **Party:** a signatory to this Agreement;
- **Patches:** a corrective Software code change issued by Supplier to the Buyer and which does not constitute a Major Release or Minor Release;
- **Permitted Use:** the Buyer's use of the Software and Software Services which is restricted to:
 - (i) the internal business requirements of the Buyer only; and
 - (ii) no other use, unless it has the prior written consent of Supplier, which the Buyer acknowledges may be subject to additional Fees if approved by Supplier;
- **Permitted Users:** the users or groups of users permitted by the Buyer to access and utilise the functionality of the Software and/or Software Service, for example, enrolled students and Learners of the Buyer;
- **Personnel:** in relation to a Party, the officers, employees, contractors (including subcontractors) and agents of that Party (but, in the case of the Buyer, excluding Supplier);
- **Platform:** the run-time software comprising Database, middle-ware and Operating Systems;
- **Platform as a Service or PaaS:** where a software platform is provided as a service in the Public Cloud;
- **Platform Management:** as set out in Annex D.3;
- **Power User Interface:** the Microsoft Windows native client application used to access the SITS:Vision or ebs Service, if applicable;
- **Priority:** A category used to identify the relative importance of an Incident, problem or change. Priority is based on impact and urgency and is used to identify required times for actions to be taken. This is the level which Supplier assigns to any issue when the Software and/or Software Service is not Available. The Priority descriptions are (i) Priority 1 or P1 or Critical Fault, (ii) Priority 2 or P2 or Major Fault, (iii) Priority 3 or P3 or Important Fault, (iv) Priority 4 or P4 or Minor Fault;
- **Proactive Monitoring:** as set out in Annex D.3, if applicable;
- **Problem:** linked Incidents that are thought to have the same underlying cause;
- **Problem Management:** process for seeking a resolution of a Problem;
- **Production Environment:** the Environment that supports the Software, Software Service, Platform and Infrastructure in which the Buyer productively conducts actual transactions in day-to-day business operations;
- **Professional Services:** consultancy services provided by Supplier to the Buyer;
- **Public Cloud:** type of computing in which a service provider makes resources available to the public via the internet;
- **Publish and Subscribe:** is a type of system to system interaction based on events where one system subscribes to be notified about an event and the other system provides a notification when that event occurs;
- **Recovery Point Objective (RPO):** is the maximum targeted period in which data (transactions) might be lost from the Software Service due to a Disaster Event;
- **Recovery Time Objective (RTO):** the duration of time within which the Software Service is targeted to be restored from Backups;
- **Registered Users:** authorised users of the Buyer, for example, stakeholders, enquirers, administrative, teaching or other staff and approved contractors (which

T R I B A L

specifically excludes any direct or indirect competitor of Supplier) and sponsors of the Buyer who have the ability to access the Software and/or Software Service;

- **Remote, Remotely:** Services performed from a location other than On Site;
- **Remote Daily Rate:** the daily professional fees for Personnel where Supplier delivers Services that are not On Site;
- **Remote Desktop Services:** accessing a software application that is not browser based remotely in a way where the software application runs remotely and the user interface is projected onto the user's local device;
- **Renewal Term:** as defined in the Agreement;
- **Reports:** includes Critical Fault Report, Major Fault Report and Root Cause Report;
- **Request:** a request made by the Buyer in accordance with this Agreement;
- **Resilience:** as set out in Annex D.3, if applicable;
- **Respond, Responded and Response:** any official communication between Supplier and the Buyer regarding an Incident, problem or change. This could include telephone, email or portal-based communications;
- **Resolution SLT:** as detailed in Annex D.1 clause 3;
- **Response SLT:** as detailed in Annex D.1, clause 3;
- **Response and Resolution:** as detailed in Annex D.1;
- **Resolution, Resolve or Resolved:** correction of a Fault or a Work Around in relation to the Fault. Priority 1 Faults may be corrected by providing a Work Around that materially restores the Services while a root cause analysis and resulting remediation is developed and implemented;
- **Restoration Request:** A Buyer enquiry to request the restoration of data from a valid Backup, snapshot or archive;
- **Restoration Requests - Response and Resolution Commitment:** as set out in Annex D.3;
- **Root Cause Report:** a report containing the following information:
 - (i) problem description;
 - (ii) background to the Incident;
 - (iii) impact summary;
 - (iv) corrective action taken;
 - (v) root cause analysis;
 - (vi) preventative actions; and
 - (vii) recommendations;
- **Scheduled Maintenance Window:** A published maintenance window for the Application of Updates, Upgrades or other changes to an Environment. A maintenance window may result in the Environment being not Available;
- **Script:** batch instructions in an appropriate software language to update or alter the Database schema;
- **Security and Compliance:** as set out in Annex D.3 and Annex D.4, as applicable;
- **Semestry SaaS:** the Software specified in Annex A, made available to Registered Users and Permitted Users as an Online Service as detailed in Annex D.6 together

TRIBAL

with the Core Support Services detailed in Annex D.1;

- **Semestry SaaS Services:** as set out in Annex D.6;
- **Service Account Plan:** a forward looking plan agreed between the Parties and updated from time to time which includes details about:
 - (i) Maintenance Window schedules;
 - (ii) Planned Upgrades; and
 - (iii) Critical periods for the Buyer including periods such as enrolment;
- **Service Desk:** the Supplier communications centre that provides a single point of contact between Supplier and its customers. The purpose of the Service Desk is to ensure that Designated Customer Support Staff receive appropriate help in a timely manner and that all Incidents and problems are escalated to higher levels of support as needed;
- **Service Downtime or SD:** the elapsed time in minutes (excluding any regular Scheduled Maintenance Windows and any Scheduled Maintenance Windows for Upgrades agreed with the Buyer) during the Service Period in which the Tribal Edge SaaS and Tribal Cloud SaaS (as applicable) is either completely unavailable to the Buyer, or the Tribal Edge SaaS and Tribal Cloud SaaS (as applicable) is partially available to the Buyer (such that it has no reasonable capacity to be used for the business purposes for which the Tribal Edge SaaS and Tribal Cloud SaaS (as applicable) was purchased, taking into account the time of such partial availability);
- **Service Engagement and Reporting:** as set out in Annex D.1;
- **Service Level – Software Service:** the level of service (Essential, Enhanced or Enterprise) applicable to the Software Service and identified in the Software Service for the Software. For clarity and by way of example, if the Service Level identified in the Software Service is Essential, then any service description in Annex D.3 marked as Enterprise will not apply and only the service description marked as Essential will apply, and vice versa. If a service is not marked as Essential, Enhanced or Enterprise, then it is applicable irrespective of the Service Level identified;
- **Service Level Target or SLT:** the estimated delivery time for a Response and/or Resolution of an Incident and as detailed in Annex D.1, Annex D.3 and Annex D.4 (as applicable);
- **Service Performance Management:** as set out in Annex D.3v and Annex D.4, as applicable;
- **Service Performance Measure:** Response time for a Synthetic Transaction from about 5 geographical locations;
- **Service Period:** a calendar month, save that:
 - (i) the first service period shall begin on the first Go Live and shall expire at the end of the calendar month in which the first Go Live falls; and
 - (ii) the final service period shall commence on the first day of the calendar month in which the Term expires or terminates and shall end on the expiry or termination of the Term;
- **Service Request Management:** the process for management of Service Requests, as set out in Annex D.1 and Annex D.3;
- **Service Request Statistics:** A set of measures related to the processing of Service Requests agreed from time to time by the Parties which may include, but are

TRIBAL

not limited to, the number of Service Requests raised in a Service Period, the number resolved and the average time for resolution;

- **Service Requests:** a request by the Buyer for an addition, change or deletion of an element of the Services;
- **Service Reviews:** as set out in Annex D.3;
- **SLT:** Service Level Target;
- **Software:** means the Software and Modules specified in the Agreement (including Major Releases or Minor Releases) but excluding any Third-Party Software;
- **Software and Service Documentation:** the instruction manuals, training manuals, user guides and other information relating to the Software (including any Major Release thereof) to be made available to the Buyer, whether printed or electronically distributed;
- **Software Service:** the service used by the Buyer to access the Software, e.g., Tribal Cloud SaaS and/or Tribal Edge SaaS and/or Tribal Dynamics SaaS and/ or Semestry SaaS used by the Buyer to access the Software, as detailed in Table 1 of Schedule 1 to the Agreement;
- **Stack:** a discreet set of Infrastructure within the Public Cloud;
- **Support Days:** as defined in Annex D.1), Annex D.3 and Annex D.4, as applicable;
- **Support Fees:** as set out in the Agreement;
- **Support Hours:** as defined in Annex D.1), Annex D.3 and Annex D.4, as applicable;
- **Support Service Procedure:** the procedure for providing Core Support Services, as set out in Annex D.1);
- **Support Services:** the support provided for the Supported Software in accordance with the Type of Support set out in the Software Service and as detailed in the corresponding Annex for that Type of Support;
- **Supported Environments:** those instances of the Software which are supported through the Support Services including the remediation of Faults, management of Availability and provision of Upgrades;
- **Supported Software:** Software which is subject to a Support Service and is not Unsupported Software;
- **Synthetic Transaction:** A transaction developed for the purposes of measuring Service Performance for example logging into the system or accessing a certain webpage in the Application;
- **Technical Configuration:** as set out in Annex D.3, as applicable;
- **Term:** as defined in the Agreement;
- **Third-Party Applications:** any software licensed by the Buyer from a third party and integrated in the Tribal SaaS and Cloud Services, as applicable;
- **Third-Party Licence:** the licence to be entered into directly between a Third-Party Proprietor and the Buyer or (as the case may be) the sub-licence to be entered into between Supplier and the Buyer in such form as may be required by the Third-Party Proprietor, for the use of Third-Party Software and/or Third-Party Application;
- **Third-Party Proprietor:** the person, firm or company who/which owns the Third-Party Software or Third-Party Application;
- **Third-Party Software:** any software (including Open Source Software) provided by Supplier in connection with this Agreement, and which is integrated into the

TRIBAL

Software, the copyright of which is not owned by Supplier;

- **Transition Support:** as set out in Annex D.3;
- **Tribal Cloud SaaS Hours:** as set out in Annex D.3;
- **Tribal Cloud SaaS Management:** as set out in Annex D.3;
- **Tribal Cloud SaaS:** the Software specified in the Software Service, made available to Registered and Permitted Users on demand via the Internet from Supplier's servers as detailed in Annex D.3 together with the Core Support Services detailed in Annex D.1;
- **Tribal Communities:** web-based searchable knowledge base, providing access to Frequently Asked Questions (FAQs), Wiki pages and a list of previously reported issues that have been identified within the versions of the Software;
- **Tribal Edge SaaS Services:** as set out in Annex D.4;
- **Tribal Edge Software As A Service or Tribal Edge SaaS:** the Software made available to Registered Users and Permitted Users as an Online Service as detailed in Annex D.4 together with the Core Support Services detailed in Annex D.1;
- **Tribal Global Service Desk:** Supplier's single customer service desk which provides Services, including Support Services for the Software and Software Services. The Global Service Desk acts as a single coordinated unit but may be distributed over more than one geographical location;
- **Tribal IPR:** any and all Intellectual Property Rights of Supplier and its Affiliates, including without limitation in the Software, Software Service, Software and Service Documentation, in the Services (including any material that Supplier creates whilst undertaking the Services) and in the Supplier brand but excludes Customer Data;
- **Tribal SaaS and Cloud Services:** means:
 - (i) Tribal Edge SaaS;
 - (ii) Tribal Dynamics SaaS;
 - (iii) Semestry SaaS; and
 - (iv) Tribal Cloud SaaS,
 as applicable to the Software Service for the Software and detailed in Table 1 of Schedule 1 to the Agreement;
- **Tribal SaaS:** means:
 - (i) Tribal Edge SaaS;
 - (ii) Tribal Edge Dynamics SaaS;
 - (iii) Semestry SaaS; and
 - (iv) Tribal Cloud SaaS,
 as applicable to the Software Service for the Software and detailed in Table 1 of Schedule 1 to the Agreement;
- **Tribal Software Support Services:** as detailed in Annex D.2;
- **Unscheduled Maintenance Window:** An unpublished change window used to apply emergency changes to an Environment in accordance with agreed Change Management processes. A maintenance window may result in the Environment being not Available;
- **Unsupported Period:** the period during which the Buyer's Production Environment is Unsupported Software;

TRIBAL

- **Unsupported Software:** Software in the Buyer's Production Environment which is not:
 - (i) **SITS:Vision:** the Major Release version of the Software released within the last 18 months;
 - (ii) **Software other than SITS: Vision:** the current release or the immediately preceding two Major Releases of Software;
- **Update:** a Minor Release of the Software and/or as set out in Annex D.3 and Annex D.4, as applicable;
- **Upgrade:** a Major Release of the Software and/or as set out in Annex D.3, Annex D.4, Annex D.5 and Annex D.6, as applicable;
- **Upstream Systems:** Buyer managed systems that feed data into Tribal SaaS and Cloud Services;
- **Usage Analysis:** as set out in Annex D.3, if applicable;
- **Usage Measures:** Measures illustrating how the Services are being used and consumed which will be updated from time to time as the Service is evolved and developed. Usage Measures may include:
 - (i) Peak and average Power User Interface usage;
 - (ii) Auto-scaling event;
 - (iii) Database volumes; and
 - (iv) e:Vision and Stu Talk transaction rates;
- **Work Around:** reducing or eliminating the impact of an Incident or problem for which the full Resolution is not yet available;
- **Working Hours:** The hours of 09:00 and 17:00 Monday to Friday excluding public holidays in the Jurisdiction and "Working Days" shall be construed accordingly.



ANNEX D.2
TRIBAL SOFTWARE SUPPORT SERVICES

3. Tribal Software Support Services Overview

1.2 This Annex describes the Tribal Software Support Services to be performed by Supplier, in respect of the Supported Software (as defined in this Annex), during the Term.

4. Key Details of Tribal Software Support Services.

Is Tribal providing Tribal Software Support Services? If No, this Annex does not apply.	Yes
Commencement Date	Effective Date unless otherwise agreed between the Parties in writing.
Supported Software and Software Service <i>NB: Not Applicable to Tribal SaaS, Semestry SaaS or Tribal Dynamics SaaS.</i>	The Software detailed in Table 1 of Schedule 1 to the Agreement where the Software Service for that Software is On Premise or Tribal Cloud SaaS (if applicable).
Support Services	The Tribal Software Support Services are supported, in the following order of precedence, with: <ul style="list-style-type: none">• Annex D.3 – Tribal Cloud SaaS;• Annex D.2 – Tribal Software Support Services; and• Annex D.1 – Core Support Services.

5. Key Details of Tribal Software Support Services.

Tribal Software Support Services	<p>The Tribal Software Support Services include:</p> <ul style="list-style-type: none">• provision of Patches, Scripts and Minor Releases (at Supplier's sole discretion), subject to the provision of the Buyer's compliance with the Release Installation Procedure; and• provision of Major Releases at no additional charge, at intervals determined solely by Supplier, subject to the Buyer's compliance with the Release Installation Procedure. <p>For the avoidance of doubt, Tribal Software Support Services do not cover:</p> <ul style="list-style-type: none">• the management and implementation of Patches, Scripts and Minor Releases except where expressly agreed in this Agreement; and• support for the Business Configuration nor any remediation of the Business
---	---



	Configuration necessary for any Update or Upgrade, except where expressly agreed in this Agreement.
Release Installation Procedure	Any and all Major Releases or Minor Releases shall be installed in a Non-Production Environment prior to the installation of the Major Releases or Minor Release into the Production Environment.
Software Fault And Usage Analytics	The Buyer agrees to Supplier automatically and regularly collecting anonymised software fault and usage analytics for the purposes of on-going software improvement. The Buyer agrees to facilitate the collection of such data.
Customer Responsibilities	Where the Software is installed on equipment controlled by the Buyer, the Buyer shall provide remote access and other necessary telecommunication facilities to enable Supplier to provide the Software Support Services remotely.

ANNEX D.3

TRIBAL CLOUD SaaS

1 Tribal Cloud SaaS

- 1.1 This Annex describes the Tribal Cloud SaaS to be provided by Supplier, in respect of the Supported Software and Software Service (as defined in this Annex), during the Term.

2 Key Details of Tribal Cloud SaaS

Are Tribal Cloud SaaS being provided? <i>If No, this Annex does not apply.</i>	Yes
Commencement Date	Effective Date unless otherwise agreed between the Parties in writing.
Supported Software and Software Service	<ul style="list-style-type: none"> The Software on the detailed in Table 1 of Schedule 1 to the Agreement where the Software Service is Tribal Cloud SaaS; and Where applicable, the Third-Party Applications detailed in Table D.3:2 (if any).
Support Services	<p>The Tribal Cloud SaaS are supported, in the following order of precedence, with:</p> <ul style="list-style-type: none"> Annex D.3 - Tribal Cloud SaaS; Annex D.2 - Tribal Software Support Services; and Annex D.1 - Tribal Core Support Services.
Support Hours / Support Days	<p>The Working Hours set out in section 4 (Definitions) of Annex D.1 when the Support Services will be provided ("Support Hours").</p> <p>Supplier will use reasonable efforts to progress Priority 1 Faults on a 24 hour by 365 day basis if the Buyer is able to make their relevant staff available on a 24 hour by 365 day basis.</p>
Service Notifications	<p>Buyer Contact Details for Proactive Service Notifications.</p> <p>Service notifications are notifications about P1 and P2 Incidents, whether raised by the Buyer or by Supplier's automated monitoring.</p> <p>Email: [REDACTED]</p> <p>Buyer Contact Details for Service Change Notifications.</p> <p>Change notifications are notifications of planned change to the Tribal Cloud SaaS which may impact the Software and/or Software Service.</p> <p>Email: [REDACTED]</p>

	The Customer shall promptly notify any changes to these contact details to Supplier.								
Cloud Type	Shared Cloud								
Cloud Region	United Kingdom								
Level of Tribal Cloud SaaS	Enhanced								
Optional Services to be Provided	<ul style="list-style-type: none"> Not applicable 								
Database Allocation	<p>The following initial Database size allocations apply to the Services:</p> <p>Table D.3:2: Database Allocation</p> <table> <tr> <th>Environment</th><th>Database</th><th>Document Storage</th></tr> <tr> <td>Production</td><td colspan="2" rowspan="2">[REDACTED]</td></tr> <tr> <td>Non-Production (in aggregate)</td></tr> </table>		Environment	Database	Document Storage	Production	[REDACTED]		Non-Production (in aggregate)
Environment	Database	Document Storage							
Production	[REDACTED]								
Non-Production (in aggregate)									
Third-Party Application	<p>The licences to Third-Party Applications agreed to be supplied by the Buyer and managed within Tribal Cloud SaaS.</p> <p>Table D.3:2: Tribal Cloud SaaS - Third-Party Applications</p> <table> <tr> <th>Third-Party Application</th><th>Third-Party Licence Terms</th><th>Volume/Limits</th></tr> <tr> <td>Not applicable</td><td>Not applicable</td><td>Not applicable</td></tr> </table>		Third-Party Application	Third-Party Licence Terms	Volume/Limits	Not applicable	Not applicable	Not applicable	
Third-Party Application	Third-Party Licence Terms	Volume/Limits							
Not applicable	Not applicable	Not applicable							
Supported Environments	<p>The following Supported Environments are provided and supported by the Tribal Cloud SaaS:</p> <p>Table D.3:3: Tribal Cloud SaaS - Supported Environments</p> <table> <tr> <th>Name of Environment</th><th>Stack containing the Environment</th><th>Description</th></tr> <tr> <td>Live</td><td>Production</td><td>An Environment in which the</td></tr> </table>		Name of Environment	Stack containing the Environment	Description	Live	Production	An Environment in which the	
Name of Environment	Stack containing the Environment	Description							
Live	Production	An Environment in which the							

			Buyer productively conducts actual transactions in day-to-day business operations.
	Test/ Dev	Enterprise and Enhanced Level: Non-Production	An Environment used for development, test and similar activities.
		Essential Level: Production	
Production Environment: Available 24x365.			
Production Support Environment: (if included): Available 24x365.			
Pre-production Environment (if included): Assumed to be active no more than 20% of the elapsed time in any Contract Year (i.e. 1,752 hours/Contract Year).			
Non-production Environment(s):			
<ul style="list-style-type: none">After Go Live Date: Available during the hours of 08:00 and 18:00 in the Jurisdiction Monday to Friday inclusive (excluding public holidays) and at other times by request up to 40% of the elapsed time in a Service Period (i.e. between 269 hours/Service Period and 298 hours per Service Period, depending on the Service Period length).Before Go Live Date: the hours of 08:00 and 18:00 in the Jurisdiction Monday to Friday inclusive (excluding public holidays) and outside these hours as necessary to deliver the migration activities (if applicable).			
Cloud Provider	Tribal Cloud SaaS is supported by a third-party Cloud Provider for Tribal Cloud SaaS. The following terms apply in relation to the Cloud Provider and its terms of service: <ul style="list-style-type: none">Cloud Provider Changes its Terms of Supply: In the event that the Cloud Provider changes its terms, Supplier reserves the right to amend this Agreement, solely to the extent necessary to reflect such changes in the Cloud Provider terms. Supplier will inform the Buyer of any such change and the effect (if any) on the Tribal Cloud SaaS. The Buyer's continued use of the Tribal Cloud SaaS, after notification of such change, will be deemed the Customer's agreement to such amended terms; andChange of Cloud Provider: Supplier may, providing it is acting reasonably and has first provided 6 months' prior written notice to the Buyer, change the Cloud Provider to a new Cloud Provider who shall have appropriate expertise and capability. Supplier must take all reasonable steps to minimise any disruption to the Tribal Cloud SaaS including that (i) any cutover is undertaken outside Working Hours, and (ii) provides a testing environment to test the Tribal SaaS and Cloud Services once migrated to the new Cloud Provider Environment.		
Assumptions	Tribal Cloud SaaS is subject to the following assumptions:		

- Unless otherwise agreed in writing between the Parties, the Buyer may only retain up to eight years' old Customer Data within the online Database or other online storage. Older data can be provided to the Customer in an industry standard read-only archive format if required. Supplier will not delete Customer Data without prior written notification to the Buyer;
- Regular Database housekeeping is undertaken to remove unnecessary data. No more than 2 years of audit data is retained in the active database. Logging and trace facilities within the Application are only used to support specific analysis and investigations that are time-limited and any log or trace data is deleted in a timely manner.
- Database and associated storage growth is no more than 5% per annum by volume. For SITS:Cloud this is on a per unit basis for the Metric Level of the Student FTE Numbers;
- The Production Environment is fully provisioned one month before Go Live, and prior to Go Live as needed for performance and penetration testing;
- For SITS:Cloud, documents managed or referred to by SITS such as, but not limited to, passport scans, transcripts etc are stored on associated storage and not in the Database;
- In line with normal SITS practice, SITS documents are provisioned on infrequent access storage which assumes read and write access is no more than three times the total amount of document storage in any Service Period;
- If applicable, the Read-only Replica Database has been sized based on current information about the expected level of activity. All interfacing and extraction, transformation, load ("**EFL**") activity is covered within the Subscription Fees specified in Schedule 2. If reporting activity against the Read-only Replica Database increases to a level that means performance does not meet the Buyer's requirements then a higher specification Read-only Replica Database server may need to be provisioned. If the Buyer determines a higher specification Database server is required then Supplier will provide a Proposal/Change Request for the additional Subscription Fees payable;
- Supplier shall not be responsible for any non-conformance where this is due to Buyer configuration or bespoke Structured Query Language ("**SQL**") (using tools such as, but not exclusively, RHI/RHQ/SQL Workbench) unless these have been agreed in writing by Supplier; and
- At least 90% of the Buyer's PowerUI Concurrent Users are located in the time zone of the Jurisdiction.

3 Description of Tribal Cloud SaaS

Tribal Cloud SaaS	<p>The scope of Tribal Cloud SaaS includes both the Application level and the Infrastructure level as detailed in this Annex.</p> <p>The Tribal Cloud SaaS does not provide management and maintenance of the Business Configuration nor any remediation of the Business Configuration necessary for any Update or Upgrade.</p> <p>For the avoidance of doubt, Tribal Cloud SaaS do not cover the Excluded Support Services.</p>
Application Management Services	<p>Tribal Cloud SaaS provides Application Management Services for the Supported Software deployed into the Supported Environments, unless otherwise stated.</p> <p>The scope of the Application Management Services includes:</p> <ul style="list-style-type: none"> • Technical Configuration; • Application Updates and Upgrades; and • Third-Party Application. <p>These Application Management Services are detailed in the below sections.</p>
	<p>Technical Configuration</p> <p>The scope of Technical Configuration is limited to the Supported Software and Software Service.</p> <p>Where applicable, Applications may be modified via back-end configuration files. Such modifications typically include the following:</p> <ul style="list-style-type: none"> • managing the Database environment; • changing user or Database connection details; • revising Application licences; • activating new Application components and services; • changing Application logging; • putting bespoke files and forms into operation; and • applying the latest assignment and configuration files. <p>NB: This service does not cover Business Configuration or customisation of the Application.</p>
	<p>Application Updates and Upgrades</p> <p>The scope of the Software Updates and Upgrades includes the Supported Software and Software Services, as follows:</p> <ul style="list-style-type: none"> • Updates: the management and deployment of any corrective Software release or

	<p>code Modification provided by Supplier per Application, per Environment. Disruptive Application Updates will be undertaken remotely outside normal Working Hours in respect of Production Environments.</p> <ul style="list-style-type: none"> • Upgrades: up to two Upgrades each year and with each Upgrade to take the Application to a version that will be supported for at least 6 months after the Upgrade is complete. Typically, a double upgrade will be undertaken once a year. Upgrades will be undertaken remotely outside Working Hours in respect of Production Environments.
	<p>Third-Party Applications</p> <p>The scope of Third-Party Applications is limited to the Third-Party Applications in Table D.3:2 only.</p> <p>If applicable, it will typically provide change management, deployment and verification of the following:</p> <ul style="list-style-type: none"> • installation, configuration and Upgrade of supported Third-Party Applications; and • updating and maintenance of supported Third-Party Applications. <p>This service is dependent on the provision and availability of new versions of the Third-Party Applications.</p>
Infrastructure Services	<p>Tribal Cloud SaaS provides Infrastructure Services for the Supported Environments in which the Application is deployed.</p> <p>The scope of the Infrastructure Services includes the provision, management and maintenance of all Infrastructure required to deliver the Tribal Cloud SaaS are:</p> <ul style="list-style-type: none"> • Platform Management; • Infrastructure Management; • Capacity Management; • Backup and Restore; and • Security and Compliance. <p>The Infrastructure Services are detailed in the below sections.</p>
	<p>Platform Management</p> <p>The scope of Platform Management is limited to the Supported Software and Software Service and includes the management of firewalls, load balancers, networks, storage systems, anti-malware systems, auto-scaling provision and monitoring systems, Databases and Operating System components.</p> <p>For Databases and Operating Systems, the service consists of:</p> <ul style="list-style-type: none"> • Database Backup and Restore Management: provides for the implementation, maintenance and monitoring of a Database Backup routine and restorations when required;

	<ul style="list-style-type: none"> • Database Administration, Monitoring and Advice: provides the day to day administration of the Databases instance, ensuring its availability and performance; • for SITS:Cloud and ebs:Cloud: Database refresh management provides the option of copying full sets of data from the Production Environment to a non-production Environment ("Non-Production Refresh"), with appropriate data masking where this can be automated to minimise privacy concerns. The service includes up to [REDACTED] with the option to purchase additional Refreshes. Each Refresh covers the extraction of data from the production Database, execution of the agreed anonymisation routines against this data and the loading of this data into up to 3 Non-Production Environments as part of the one Non-Production Refresh. For SITS:Cloud, refreshes from the Production Environment to either a Pre-Production Environment or a Production Support Environment can be provided. If the Production Support Refreshes can be automated t [REDACTED] r. • Operating System administration, maintenance and management: provides for the following activities: <ul style="list-style-type: none"> ○ system service and process maintenance; ○ stopping/starting/restarting services; ○ terminating processes; ○ application log rotation; ○ local user account administration; ○ Cron and scheduled task management; ○ server, database and infrastructure level access is not provided to the Buyer except for one data migration Database during the implementation period and the Read-only Replica Database option where direct SQL read access can be provided.
	<p>Infrastructure Management</p> <p>The scope of Infrastructure Management is limited to the provision and management of the Infrastructure required for the Tribal Cloud SaaS from the point of ingress to the Cloud Provider from the Internet to the point of egress from the Cloud Provider to the Internet.</p> <p>The Operating System and pre-requisite components will be maintained at the level the Tribal Cloud SaaS needs to operate. The Supported Environments covered are detailed in this Annex.</p> <p>Updates (including Patches) to the Operating System are undertaken based on the advice of the Operating System provider (reviewed by Supplier) and are installed in accordance with Change Management practices through the designated Non-Production Environments prior to application into the Production Environment within an appropriate Scheduled Maintenance Window.</p> <p>Disruptive Updates are undertaken outside Working Hours where these will impact the Availability of the Tribal Cloud SaaS unless an emergency or security patch needs to be</p>

	<p>applied, in which case Supplier will seek to provide the Buyer with as much advance notice as practical.</p> <p>Upgrades are undertaken outside Working Hours where these will impact the Availability of the Tribal Cloud SaaS production Environment.</p>
	<p>Capacity Management</p> <p>The scope of Tribal Cloud SaaS is to provide sufficient capacity to meet the reasonable use of the Software Service by the Buyer for the business purpose for which the Service was purchased.</p> <p>For SITS:Cloud, this will normally be met through autoscaling of the Infrastructure in response to increased demand. For ebs:Cloud and Maytas:Cloud this will normally be met through manual scaling of the Infrastructure in response to increased demand.</p> <p>Supplier will work with the Buyer to ensure sufficient capacity is provisioned to meet reasonable cyclical increases in demand, such as for results announcement or enrolment and module selection.</p>
	<p>Backup and Restore</p> <p>The scope of Backup and Restore is limited to Customer Data stored within a Database, on file systems or other alternative storage mechanisms in the Supported Environments.</p> <p>Backup</p> <p>Database transactional backups are taken transparently in the background every hour (RPO) and are retained for 35 calendar days.</p> <p>Daily Backups of Customer Data stored outside of Databases are performed transparently every 24 hours (RPO) and retained for 35 calendar days.</p> <p>Restore</p> <p>Restoration of a Database to a specific point-in-time can be performed within the 35 calendar day retention period by making a Request. This provides a Database RPO of up to an hour and an RTO of 24 hours.</p> <p>Restoration of Customer Data stored outside the Database can be performed within the 35 calendar day retention period by making a Request. This provides an RPO of up to 24 hours and an RTO of 24 hours.</p> <p>Where the Production Environment Extended Archive Retention optional service has been purchased, then copies of the monthly backups will be archived within the cloud environment for a period of 7 years or the term of the Agreement whichever is less.</p>
	<p>Security and Compliance</p> <p>The scope of Security and Compliance is limited to the provision and management of cloud-based security facilities for the Supported Environments.</p> <p>The service includes:</p>

	<ul style="list-style-type: none"> • anti-malware; • intrusion prevention; • automated vulnerability testing; • host firewall; and • web reputation. <p>Supplier will monitor events raised by the cloud-based security facilities and Respond to Alerts in accordance with the SLTs in the applicable Annexures (applying the order of precedence stated above).</p>
Tribal Cloud SaaS Management	<p>The scope of Tribal Cloud SaaS Management is:</p> <ul style="list-style-type: none"> • Service Performance Management; • Environment Monitoring; • Incident Management and Problem Management; • Change Management; and • Service Request Management. <p>The Tribal Cloud SaaS Management services are detailed in the below sections.</p>
	<p>Service Performance Management</p> <p>The scope of Service Performance Management includes Supplier collaborating with the Buyer to improve the performance of the Tribal Cloud SaaS during the Term to meet the evolving needs of the users of the Software Service and to ensure the Software Service continues to meet the business purpose for which the Software Service was purchased.</p>
	<p>Environment Monitoring</p> <p>The scope of Environment Monitoring is limited to the provision of monitoring for the Supported Environments.</p> <p>The Supported Environments will be monitored 24 hour by 365 day basis using Supplier's monitoring tools.</p> <p>Each monitored item is configured with a set of thresholds for warnings, errors and critical Alerts. When a threshold is breached, an automated email is triggered to the Service Desk where it will be managed as an Incident in accordance with the SLTs in the applicable Annexures (applying the order of precedence stated above). Supplier monitors the backup schedules as part of this service.</p>
	<p>Incident Management and Problem Management</p> <p>The scope of Incident Management and Problem Management is that Supplier will investigate and seek to resolve issues that are technical in nature, including responding to events (Alerts from monitoring).</p>

	<p>This includes the following Services:</p> <ul style="list-style-type: none"> • management and escalation of any Incidents; • management of Critical and Major Faults ensuring they are resolved promptly, maintaining Buyer communications throughout, including the production of a Critical or Major Fault Report; • monitoring Alerts analysis, resource gathering and investigation of Application and Managed Platform log files, forms and web files for support queries, setup and configuration inspections.
	<p>Change Management</p> <p>The scope of Change Management is to manage changes to a Supported Environment, for example, due to a Request or Incident resolution either by configuration, patching or Upgrade in a managed way. Where possible and practical, changes are applied to a Non-Production Environment and successfully tested before application to the Production Environment.</p> <p>The Parties will seek to align change management processes where this is practical, and are handled in the following manner and in accordance with the control points agreed with the Buyer prior to being applied to the Production Environment:</p> <ul style="list-style-type: none"> • Emergency Changes – changes that are applied at times outside Scheduled Maintenance Windows because of time or business critical or security related Incidents or Service Requests. Supplier will seek to agree a suitable time with the Buyer for the application of the Emergency Change where this is practical given the urgency of the change; • Pre-approved Changes - are changes to the Application that have the change process pre-approved and are undertaken as necessary within a Scheduled Maintenance window or at another time if they are non-disruptive; • Patches - are minor changes to the Application and are generally undertaken during a Scheduled Maintenance Window or at another time if they are non-disruptive; • Updates - are changes to the Application that do not result in updating to another Major Release and these are applied at a time agreed with the Buyer and normally during a Scheduled Maintenance Window; and • Upgrades - are changes where the Application is upgraded from one Major Release to another Major Release and will be undertaken at a time agreed with the Buyer, normally during a Scheduled Maintenance Window which is designated for Upgrades. <p>Other changes and changes to the Managed Platform, including Upgrades or Supplier or supplier approved patches, will be undertaken in the background. Changes that are expected to be disruptive to the Production Environment will be applied outside Working Hours and where possible during a Scheduled Maintenance Window. Where a change is material and will be disruptive to Other Systems, then Supplier shall provide at least three (3) months' notice.</p>

	<p>Service Request Management</p> <p>The scope of Service Request Management is to monitor and manage the fulfilment of valid Service Requests and provide regular updates and Restoration Requests in accordance with the SLTs in the applicable Annexures (applying the order of precedence stated above).</p> <p>Supplier will provide the following services:</p> <ul style="list-style-type: none"> • Management of any Service Requests and the Change Management processes.
Continuous Service Improvement	<p>The scope of Continuous Service Improvement is to regularly update the Tribal Cloud SaaS to provide access to new features and functionality or to address known issues.</p> <p>The Buyer must use supported methods of integration with the Tribal Cloud SaaS, as may be published by Supplier from time to time.</p> <p>Supplier will act reasonably to minimise the impact of such changes on the Customer.</p>
<p>Extended Archive Retention</p> <p><i>(Enterprise optional service – only applies if selected)</i></p>	<p>Recovered copies of the backups will be provided to the Buyer upon written request. The format of the backup files will enable the Buyer to load the data into a Database of the same type used in the Tribal Cloud SaaS Supported Environment. If required, Supplier can provide a quote for mounting the data in a Tribal Cloud SaaS Supported Environment and providing access.</p>
Resilience	<p>To the extent that the Supported Software is able to support Resilience and High Availability, the scope of Resilience is to provide High Availability (HA) resilience for Production instances, including:</p> <ul style="list-style-type: none"> • multiple Availability Zone (AZ) deployment where this is offered by the Cloud Provider in the Cloud Region <i>(Enterprise and Enhanced Level only)</i>; • AZ redundant Platform as a Service (PaaS) such as Relational Database Services (RDS) <i>(Enterprise and Enhanced Level only)</i>; • running of multiple instances for the webapp/integration/client tier; • segregation of webapp/integration/client tier; • load balancer with health checks; • load based auto scaling of compute for WebApp and integration middleware; and • auto-recovery for batch and Power User Interface middleware compute.
<p>Transition Support</p> <p><i>(Enterprise Level)</i></p>	<p>The scope of Transition Support is provide to the Buyer a Technical Lead (“TL”) as the point of contact for all technical requirements to facilitate the deployment and transition from project initiation to BAU of the Tribal Cloud SaaS.</p> <p>The TL will:</p> <ul style="list-style-type: none"> • be assigned at the commencement of the implementation;

	<ul style="list-style-type: none"> • provide technical leadership of the Cloud installation and implementation; • be responsible for planning and co-ordination of all technical activities that relate to the delivery of cloud-based system implementation of the Software; • ensure all technical project deliverables are clearly defined, documented, scheduled and delivered to project milestones; and • documenting and communicating agreed processes and procedures between the Customer and Supplier.
Engagement Services	<p>The scope of Engagement Services for the Supported Software Service and Environments includes:</p> <ul style="list-style-type: none"> • Customer Success Manager (CSM); • Service Engagement; • Proactive Monitoring; and • Usage Analysis. <p>The Engagement Services are detailed in the below sections.</p>
	<p>Customer Success Manager</p> <p>A Customer Success Manager (“CSM”) will be assigned to the Buyer no later than one month before the transition to BAU. The CSM will be responsible for providing the following services in BAU:</p> <ul style="list-style-type: none"> • assist with escalation of any problems with Upgrades or Updates; • coordinate Upgrades in collaboration with Buyer requirements; • act as liaison during any Major or Critical Faults, maintaining Buyer communications throughout, including the production of a Root Cause Report; • deliver Buyer Service Reviews; and • provide Cloud Service Health and Performance Report for each Service Period.
	<p>Service Engagement (<i>Enterprise and Enhanced Level</i>)</p> <p>The scope of Service Engagement is to provide the Buyer with online Cloud Service Health and Performance Reports for each Service Period and monthly Service Reviews in relation to the Supported Software and Software Services.</p> <p>The purpose of the Service Reviews is (where applicable) to achieve the following:</p> <ul style="list-style-type: none"> • to review the Cloud Service Health and Performance Report; • to agree and/or review the Service Account Plan; • understand, review and plan future Service Requests and agreeing dates for Upgrades;

	<ul style="list-style-type: none"> • to communicate the following; <ul style="list-style-type: none"> ○ the root cause analysis for P1 Incidents that have been closed since previous Service Review; and ○ progress on any outstanding P1 Incidents; ○ an update on any outstanding Problems. <p>The service review will be attended by the CSM who may be supported by a Technical representative, where appropriate.</p>
	<p>Service Engagement (<i>Essential Level</i>)</p> <p>The scope of Service Engagement is to provide the Buyer with online Cloud Service Health and Performance Report for each Service Period and annual Service Reviews in relation to the Supported Software and Software Services.</p> <p>The purpose of the Service Reviews is (where applicable) to achieve the following;</p> <ul style="list-style-type: none"> • to review the Cloud Service Health and Performance Report; and • to agree and/or review the Service Account Plan. • understand, review and plan future Service Requests and agreeing dates for Upgrades; • to communicate the following; <ul style="list-style-type: none"> ○ the root cause analysis for P1 Incidents that have been closed since previous Service Review; and ○ progress on any outstanding P1 Incidents; ○ an update on any outstanding Problems. <p>The service review will be attended by the CSM who may be supported by a Technical representative, where appropriate.</p>
	<p>Proactive Monitoring</p> <p>The scope of Proactive Monitoring is to provide a level of monitoring and analysis for Applications and Infrastructure.</p> <p>The service allows the Designated Tribal Personnel to proactively monitor KPIs for impact on Availability. Proactive Monitoring is conducted to prevent Incidents from occurring. The Tribal Cloud SaaS is configured to monitor the following:</p> <ul style="list-style-type: none"> • threshold warnings, errors and critical alerts; • log files, forms and web files for support queries; and • performance measures and system benchmarks.
	<p>Usage Analysis (<i>Enterprise Level</i>)</p> <p>The scope of Usage Analysis is to provide information on the level of adoption of different</p>

	aspects of the Tribal Cloud SaaS, including regular feedback to indicate the levels of utilisation and consumption of the different user access methods, overall numbers of users and batch processing.						
Service Engagement and Reporting -Critical and Major Incident <i>(Enterprise Level)</i>	<p>The scope of Service Engagement and Reporting includes communication during the Resolution of Critical and Major Faults in the Supported Environments, as detailed in Table D.3:4 and Table D.3:5.</p> <p>It includes the provision of the following reports (as applicable):</p> <ul style="list-style-type: none"> • Critical Fault Report; • Major Fault Report; and • Root Cause Report. <p>Depending on the nature of the Fault and the time needed to determine the root cause, the Root Cause Report may be combined with the Critical Fault Report or the Major Fault Report.</p> <p>The Report Timeframes set out in Table D.3:4 and Table D.3:5 are estimates and wherever possible, a Report will be provided more quickly.</p>						
	<p>Table D.3:4: Tribal Cloud SaaS - Critical Fault (Priority 1) events and reporting</p> <table> <tr> <th>Report Timeframes</th><th>Report</th></tr> <tr> <td>After initial triage and diagnosis</td><td>If the Resolution is clear and straightforward, then the Resolution will be actioned. If not, a Major Incident Team will be assembled, and a MI Manager will be appointed. The Buyer will be provided with the MI Manager name and contact details.</td></tr> <tr> <td>Enhanced and Essential Level: Within 1 Support Hour</td><td> <p>The initial triage will provide the following information via Customer Portal:</p> <ul style="list-style-type: none"> • case number; • Incident date and time; • Buyer contact details; • Software version details; • a problem statement; • a business impact assessment; </td></tr> </table>	Report Timeframes	Report	After initial triage and diagnosis	If the Resolution is clear and straightforward, then the Resolution will be actioned. If not, a Major Incident Team will be assembled, and a MI Manager will be appointed. The Buyer will be provided with the MI Manager name and contact details.	Enhanced and Essential Level: Within 1 Support Hour	<p>The initial triage will provide the following information via Customer Portal:</p> <ul style="list-style-type: none"> • case number; • Incident date and time; • Buyer contact details; • Software version details; • a problem statement; • a business impact assessment;
Report Timeframes	Report						
After initial triage and diagnosis	If the Resolution is clear and straightforward, then the Resolution will be actioned. If not, a Major Incident Team will be assembled, and a MI Manager will be appointed. The Buyer will be provided with the MI Manager name and contact details.						
Enhanced and Essential Level: Within 1 Support Hour	<p>The initial triage will provide the following information via Customer Portal:</p> <ul style="list-style-type: none"> • case number; • Incident date and time; • Buyer contact details; • Software version details; • a problem statement; • a business impact assessment; 						

	Enterprise Level - Within 1 clock hour.	<ul style="list-style-type: none"> • a description of the symptoms experienced; • any steps identified to reproduce the problem; • reference to evidence such as log files or screen shots to support reasoning; and • reference to any significant changes that have been carried out prior to the Incident occurring. <p>Customer Portal updates will continue to be provided in real time which will automatically notify to the Customer by email.</p> <p>Further updates will be provided on an on-going basis, typically via email or a telephone call.</p>
	Major incident management	<p>An Incident Bridge will be opened using Microsoft Teams or other suitable technology. The Incident Bridge will allow for continuous monitoring of the technical plan and Buyer staff will be added to the Incident Bridge as required.</p> <p>A technical plan of action will be communicated which will typically include:</p> <ul style="list-style-type: none"> • technical steps to Resolve Incident or provide a Work Around; • contingencies if steps do not Resolve the Incident; • timeframes for each step; • an indication of any downtime or loss of service; and • Buyer approvals and/or actions required to undertake recovery. <p>Additional steps and plans will be discussed and communicated until the Incident has been Resolved or a Work Around provided.</p>
	Further escalation as required	The Incident will be escalated internally within Supplier as required including to product development and other teams necessary to investigate and remediate.
	Within 4 Support Days	A Root Cause Report will be provided to the extent that the necessary information is available.

Table D.3:5: Tribal Cloud SaaS - Major Fault (Priority 2) Report

Report Timeframes	Report
After initial triage and diagnosis	If Resolution is clear and straightforward, then the Resolution will be actioned. If not, then an Incident manager will be assembled and they will manage the Incident through to resolution.
Within 2 Support Hours.	<p>The initial triage will provide the following information via the Customer Portal:</p> <ul style="list-style-type: none"> • Case number; • Incident date and time; • Buyer contact details; • Software version details; • a problem statement; • a business impact assessment; • a description of the symptoms experienced; • any steps identified to reproduce the problem; • reference to evidence such as log files or screen shots to support reasoning; and • reference to any significant changes that have been carried out prior to the incident occurring. <p>Customer Portal updates will continue to be provided in real time which will automatically notify to the Buyer by email.</p>
Major fault management	<p>An Incident Bridge may be opened as required using Microsoft Teams or other suitable technology. The Incident Bridge will allow for continuous monitoring of the technical plan and Buyer staff will be added to the Incident Bridge as required.</p> <p>A technical plan of action will be communicated which will typically include:</p> <ul style="list-style-type: none"> • technical steps to Resolve Incident or provide a Work Around; • contingencies if steps do not Resolve the Incident; • timeframes for each step;

		<ul style="list-style-type: none"> an indication of any downtime or loss of service; and Buyer approvals and/or actions required to undertake recovery. <p>Additional steps and plans will be discussed and communicated until the Incident has been Resolved or a Work Around provided.</p>
	Further escalation as required	The Incident will be escalated internally within Supplier as required including to product development and other teams necessary to investigate and remediate.
	Within 7 Support Days	A Root Cause Report will be provided where this is warranted and to the extent that the necessary information is available.
Customer Responsibilities	<p>Customer Responsibilities include:</p> <ul style="list-style-type: none"> ensuring that the Production Environment uses Supported Software unless this is not possible due to the action or omissions of Supplier; using supported methods of integration with the Tribal Cloud SaaS, as may be published by Tribal from time to time; for SITS:Cloud, not using SITS RQH/RQI and other direct SQL tools in the Environments without the prior written agreement of Supplier (which will not be unreasonably withheld or delayed); obtaining Supplier's prior written agreement (which shall not be unreasonably withheld or delayed) before the Buyer (or any contracted third party) undertakes performance or penetration testing against the Tribal Cloud SaaS. In the event that consent is granted it will be conditional on the full results being provided to Supplier as soon as reasonably possible on completion of the testing; not seeking to interfere with any of the Infrastructure or Environments that are managed by Supplier; providing network connectivity between user access devices and the internet; acting reasonably in its use of an Application Programming Interface (API) and use APIs for the purposes for which they were designed; provision of satisfactory licences for any Third-Party Applications to be provided by the Buyer; provision of resources to test a new version of the Application when this is required for Upgrades or Updates; and undertaking changes to systems not maintained and managed by Supplier when 	

	this is required as part of an Upgrade or Update of the Infrastructure or the Application.
--	--

4 **Specific Service Levels for Tribal Cloud SaaS**

Tribal Cloud SaaS Levels	<p>The Tribal Cloud SaaS Levels, in relation to the provision of the Supported Environments encompass:</p> <ul style="list-style-type: none">• Incident Response and Resolution;• •Restoration Requests Response and Resolution;• •Availability;• •Disaster Recovery; and• •Scheduled Maintenance Windows. <p>The Tribal Cloud SaaS Levels are detailed in the below sections.</p>												
	<p>Incident Response and Resolution (<i>Enterprise Level</i>):</p> <p>Tribal shall use Commercially Reasonable Efforts to achieve the stated Service Level Targets in respect of the Responses and Resolutions. Wherever possible, a Response or Resolution will be provided more quickly although the times indicated are targets. For clarity, SLTs only apply within the Support Hours unless otherwise specified in this Agreement.</p> <p>The following table details the SLTs for the Production Environment:</p> <p>Table D.3:6: Tribal Cloud SaaS - Service Level Targets</p> <table><tr><th>Fault Type</th><th>Response SLT</th><th>Resolution SLT</th><th>Typical Resolution Objectives</th></tr><tr><td>Critical Fault (Priority 1)</td><td>30 clock minutes</td><td>4 clock hours</td><td>To provide a Fault correction or reasonable Work Around. Resolution may involve restarting the Software or Software Service, alterations to the configuration of the Production Environment, a restore from a previous version, or the application of a fix to a previously reported issue.</td></tr><tr><td>Major Fault (Priority 2)</td><td>1 Support Hour</td><td>3 Support Days</td><td>To provide a Fault correction or reasonable Work Around. Corrective Resolution may involve restarting the Software or Software Service, or a restore from a previous ver-</td></tr></table>	Fault Type	Response SLT	Resolution SLT	Typical Resolution Objectives	Critical Fault (Priority 1)	30 clock minutes	4 clock hours	To provide a Fault correction or reasonable Work Around. Resolution may involve restarting the Software or Software Service, alterations to the configuration of the Production Environment, a restore from a previous version, or the application of a fix to a previously reported issue.	Major Fault (Priority 2)	1 Support Hour	3 Support Days	To provide a Fault correction or reasonable Work Around. Corrective Resolution may involve restarting the Software or Software Service, or a restore from a previous ver-
Fault Type	Response SLT	Resolution SLT	Typical Resolution Objectives										
Critical Fault (Priority 1)	30 clock minutes	4 clock hours	To provide a Fault correction or reasonable Work Around. Resolution may involve restarting the Software or Software Service, alterations to the configuration of the Production Environment, a restore from a previous version, or the application of a fix to a previously reported issue.										
Major Fault (Priority 2)	1 Support Hour	3 Support Days	To provide a Fault correction or reasonable Work Around. Corrective Resolution may involve restarting the Software or Software Service, or a restore from a previous ver-										

			sion, or the application of a fix to a previously reported issue.
Important Fault (Priority 3)	4 Support Hours	20 Support Days	This Priority level has a Work Around available.
Minor Fault (Priority 4)	8 Support Hours	No SLT Commitment	This Priority level has a Work Around available and may involve the issue of an Update.

For Incidents related to Tribal Cloud SaaS:

- Supplier will use reasonable efforts to progress the resolution of P1 Incidents on a 24 hour by 365 day basis subject to the Buyer being able to provide staff who are able to provide input to the Resolution on the same 24 hour by 365 day basis.
- All other Priority Incidents will be supported during Support Hours. Where these arise outside the Support Hours, the Response SLT and Resolution SLT start times (for the purpose of calculating Response and Resolution targets) will begin from the start of the next Support Hours period after the Incident is notified to Supplier.
- These service levels will not apply where the root cause of an incident is within the Public Cloud environment and Tribal can demonstrate the root cause is outside Supplier's control.
- Where the resolution of an Incident requires a software change or patch, it may not be possible to achieve the stated service levels.

Incident Response and Resolution (*Enhanced and Essential Level*):

Supplier shall use Commercially Reasonable Efforts to achieve the stated Service Level Targets in respect of the Responses and Resolutions. Wherever possible, a Response or Resolution will be provided more quickly although the times indicated are targets. For clarity, SLTs only apply within the Support Hours unless otherwise specified in this Agreement.

The following table details the SLTs for the Production Environment:

Table D.3:7: Tribal Cloud SaaS - Service Level Targets

Fault Type	Response SLT	Resolution SLT	Typical Resolution Objectives
Critical Fault (Priority 1)	30 minutes during the	4 Support Hours	To provide a Fault correction or reasonable Work Around. Resolution may involve restarting the

		Support Day		Software or Software Service, alterations to the configuration of the Production Environment, a restore from a previous version, or the application of a fix to a previously reported issue.
	Major Fault (Priority 2)	1 Support Hour	3 Support Days	To provide a Fault correction or reasonable Work Around. Corrective Resolution may involve restarting the Software or Software Service, or a restore from a previous version, or the application of a fix to a previously reported issue.
	Important Fault (Priority 3)	4 Support Hours	20 Support Days	This Priority level has a Work Around available.
	Minor Fault (Priority 4)	8 Support Hours	No SLT Commitment	This Priority level has a Work Around available and may involve the issue of an Update.
	<p>For Incidents related to Tribal Cloud SaaS:</p> <ul style="list-style-type: none"> All Priority Incidents will be supported during Support Hours. Where these arise outside the Support Hours, the Response SLT and Resolution SLT start times (for the purpose of calculating Response and Resolution targets) will begin from the start of the next Support Hours period after the Incident is notified to Supplier. These service levels will not apply where the root cause of an incident is within the Public Cloud environment and Tribal can demonstrate the root cause is outside Supplier's control. Where the resolution of an Incident requires a software change or patch, it may not be possible to achieve the stated service levels. 			
	<p>Restoration Requests Response and Resolution:</p> <p>Supplier will respond to Restoration Requests and use Commercially Reasonable Efforts to achieve the stated Service Level Targets in respect of the Responses and Resolutions. Wherever possible, a Response or Resolution will be provided more quickly although the times indicated are targets. For clarity, SLTs only apply within the Support Hours.</p> <p>The following table details the SLTs for the live Production Environment:</p> <p>Table D.3:8: Tribal Cloud SaaS - Service Level Targets - Restoration Request</p>			

	Type	Response SLT	Resolution SLT	Typical Resolution Objectives
	Restoration Request	1 Support Hour	8 Support Hours	Restoration Request

Availability:

The Tribal Cloud SaaS provides Availability for the Software and/or Software Service operating in the live Production Environment as follows:

Table D.3:9: Tribal Cloud SaaS – Availability

Service Level	Availability
Enhanced and Enterprise Level	99.9%
Essential Level	99.5%

The Availability is calculated as follows:

- Availability = $(OT - SD) / OT \times 100\%$;
 - “OT”: Operational Time;
 - “SD”: Service Downtime.

Availability is measured at the ingress point to the Production Environment from the Internet.

Disaster Recovery:

Within the Cloud Region, Disaster Recovery will be in accordance with the Disaster Recovery Plan and will include the following Recovery Point Objective (RPO) and Recovery Time Objective (RTO) targets:

Table D.3:10: Tribal Cloud SaaS - Disaster Recovery Targets

Recovery Point Objective (RPO)	Recovery Time Objective (RTO)
As set out in Backup and Restore	24 elapsed hours

Scheduled Maintenance Windows:

Scheduled Maintenance Windows can be:

- Regular Scheduled Maintenance Windows:** will take no more than 8 hours per month and will take place outside Working Hours. As part of the onboarding process, the Buyer will be allocated a weekly Scheduled Maintenance Window. Where this needs to be changed from time to time, Supplier will, acting reasonably,

	<p>allocate an amended Window to the Buyer.</p> <ul style="list-style-type: none">• Scheduled Maintenance Windows for Upgrades: will be agreed with the Buyer from time to time to Upgrade the Software to ensure it remains compliant with this Agreement.
--	--

)