



Crown  
Commercial  
Service

---

**Call Off Order Form for Management Consultancy Services**

---

## PART 1 – CALL OFF ORDER FORM

### SECTION A

This Call Off Order Form is issued in accordance with the provisions of the Framework Agreement for the provision of support to the LAs in the *Strengthening Families, Protecting Children* to successfully implement complex whole-system change projects in children's social care, dated 2 March 2020.

The Supplier agrees to supply the Services specified below on and subject to the terms of this Call Off Contract.

For the avoidance of doubt this Call Off Contract consists of the terms set out in this Call Off Order Form and the Call Off Terms.

<b>Order Number</b>	<b>TBC</b>
<b>From</b>	The Secretary of State for Education whose Head Office is at Sanctuary Buildings, Great Smith Street, London, SW1P 3BT <b>("CUSTOMER")</b>
<b>To</b>	Mutual Ventures Limited 2-6 Boundary Row London SE1 8HP <b>("SUPPLIER")</b>

### SECTION B

#### CALL OFF CONTRACT PERIOD

<b>1.1.</b>	<b>Commencement Date:</b> 2 March 2020
	<b>Expiry Date:</b>  End date of Initial Period: 31 March 2024  End date of Extension Period: 31 March 2024, with the possibility of a further extension subject to budgetary approvals.  Minimum written notice to Supplier in respect of extension: 30 days

#### SERVICES

<b>2.1.</b>	<p><b>Services required:</b></p> <p>Set out in Section 2 (Services offered) of the Framework Agreement and refined by the Customer's Project Specification attached at Annex E and the Supplier's Proposal attached at Annex F.</p>
-------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## PROJECT PLAN

<b>3.1.</b>	<p><b>Project Plan:</b></p> <p>An initial delivery plan from the Supplier is attached at Annex A. KPIs to be used during full programme delivery are also included in Annex A.</p> <p>The Supplier shall provide the Customer with a detailed project plan for approval within 60 Working Days from the Call Off Commencement Date.</p>
-------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## CONTRACT PERFORMANCE

<b>4.1.</b>	<p><b>Standards:</b></p> <p>N/A – see Clause 11 (Standards) in the Call Off Terms</p>
<b>4.2</b>	<p><b>Service Levels/Service Credits:</b></p> <p>Not applied</p>
<b>4.3</b>	<p><b>Critical Service Level Failure:</b></p> <p>Not applied</p>
<b>4.4</b>	<p><b>Performance Monitoring:</b></p> <p>Monthly contract management meetings and formal six-month contract reviews.</p>
<b>4.5</b>	<p><b>Period for providing Rectification Plan:</b></p> <p>In Clause 39.2.1(a) of the Call Off Terms.</p>

## PERSONNEL

<b>5.1</b>	<p><b>Key Personnel:</b></p> <ul style="list-style-type: none"> <li>• David Fairhurst (Engagement Director)</li> <li>• Heather Rolinson (Innovation Director)</li> <li>• Ewan King (Learning Director)</li> <li>• William Carruthers (Engagement Manager)</li> <li>• Vicky Purewal (Innovator Coach – Hertfordshire)</li> </ul>
------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<ul style="list-style-type: none"> <li>• Siobhan Edwards (Innovator Coach – North Yorkshire)</li> <li>• Prof Peter Marsh (Innovator Coach – Leeds)</li> <li>• Alissa Davies (Adopter Coach – Hertfordshire)</li> <li>• Hannah Jackson (Adopter Coach – North Yorkshire)</li> <li>• Laura Power (Adopter Coach – Leeds)</li> <li>• Nimal Jude (Learning Manager)</li> <li>• Lucy Ashlee-Williams (DfE, Contract Manager)</li> <li>• Helen Grimes (DfE, Senior Contract Manager)</li> </ul>
<b>5.2</b>	<p><b>Relevant Convictions</b> (Clause 28.2 of the Call Off Terms):</p> <p>See Clause 28.2</p>

## PAYMENT

<b>6.1</b>	<p><b>Call Off Contract Charges</b> (including any applicable discount(s), but excluding VAT):</p> <p><b>Total overall costs (charges to DfE) from 2 March 2020 to 31 March 2024</b></p> <table> <tr> <td>Total fees and expenses (exc. VAT)</td> <td style="text-align: right;">£2,464,030</td> </tr> <tr> <td>VAT</td> <td style="text-align: right;">£492,806</td> </tr> <tr> <td>Total fees and expenses (inc. VAT)</td> <td style="text-align: right;">£2,956,836</td> </tr> </table>	Total fees and expenses (exc. VAT)	£2,464,030	VAT	£492,806	Total fees and expenses (inc. VAT)	£2,956,836
Total fees and expenses (exc. VAT)	£2,464,030						
VAT	£492,806						
Total fees and expenses (inc. VAT)	£2,956,836						
<b>6.2</b>	<p><b>Payment terms/profile</b></p> <p><b>Forecast and payment profile</b></p> <p>Forecast and payment profile from the Supplier is attached at Annex B.</p> <p><b>Method of payment</b></p> <p>Invoices will be presented on a monthly basis with payment to be made within 30 days via BACS to the following account:</p> <p>Account: Mutual Ventures Limited  Bank branch: HSBC, 60 Fenchurch Street, London EC3M 4BA  Sort Code: 40 01 04  Account Number: 01823019</p>						
<b>6.3</b>	<p><b>Reimbursable Expenses:</b></p> <p>Not permitted</p>						
<b>6.4</b>	<p><b>Customer billing address</b> (paragraph 7.6 of Call Off Schedule 3 (Call Off Contract Charges, Payment and Invoicing)):</p> <p>Department for Education  Sanctuary Buildings  Great Smith Street  London  SW1P 3BT</p>						

<b>6.5</b>	<b>Call Off Contract Charges fixed for</b> (paragraph 8.2 of Schedule 3 (Call Off Contract Charges, Payment and Invoicing)): Four Call Off Contract Years and one month from the Call Off Commencement Date
<b>6.6</b>	<b>Supplier periodic assessment of Call Off Contract Charges</b> (paragraph 9.2 of Call Off Schedule 3 (Call Off Contract Charges, Payment and Invoicing)) will be carried out on: Charges are fixed until 31 March 2024.
<b>6.7</b>	<b>Supplier request for increase in the Call Off Contract Charges</b> (paragraph 10 of Call Off Schedule 3 (Call Off Contract Charges, Payment and Invoicing)): Not Permitted.

## LIABILITY AND INSURANCE

<b>7.1</b>	<b>Estimated Year 1 Call Off Contract Charges:</b> The sum of £67,062 (including expenses and VAT)
<b>7.2</b>	<b>Supplier's limitation of Liability</b> (Clause 37.2.1 of the Call Off Terms); In Clause 37.2.1 of the Call Off Terms
<b>7.3</b>	<b>Insurance</b> (Clause 38.3 of the Call Off Terms): The cover that Mutual Ventures have is as follows: Professional indemnity £5m Public Liability £10m Employers Liability £10m

## TERMINATION AND EXIT

<b>8.1</b>	<b>Termination on material Default</b> (Clause 42.2.1(c) of the Call Off Terms): In Clause 42.2.1(c) of the Call Off Terms
<b>8.2</b>	<b>Termination without cause notice period</b> (Clause 42.7.1 of the Call Off Terms): In Clause 42.7.1 of the Call Off Terms
<b>8.3</b>	<b>Undisputed Sums Limit:</b> In Clause 43.1.1 of the Call Off Terms
<b>8.4</b>	<b>Exit Management:</b> Not applied

## SUPPLIER INFORMATION

<b>9.1</b>	<b>Supplier's inspection of Sites, Customer Property and Customer Assets:</b> Not applied
<b>9.2</b>	<b>Commercially Sensitive Information:</b> Not applied

## OTHER CALL OFF REQUIREMENTS

<b>10.1</b>	<b>Recitals</b> (in preamble to the Call Off Terms)
<b>10.2</b>	<b>Call Off Guarantee (Clause 4 of the Call Off Terms):</b> Not required
<b>10.3</b>	<b>Security:</b> Short form security requirements (paragraphs 1 to 5 of Schedule 7 (Security)) AND Security Policy and Department for Education Security Standards – see Annex C.  The Supplier shall provide the Customer with a security management plan within 30 working days from the Call Off Commencement Date.
<b>10.4</b>	<b>ICT Policy:</b> Not applied
<b>10.5</b>	<b>Testing:</b> Not applied
<b>10.6</b>	<b>Business Continuity &amp; Disaster Recovery:</b> In Call Off Schedule 8 (Business Continuity and Disaster Recovery)  The Supplier shall provide the Customer with a business continuity and disaster recovery plan within 30 working days from the Call Off Commencement Date.  <b>Disaster Period:</b> For the purpose of the definition of “Disaster” in Call Off Schedule 1 (Definitions) the “Disaster Period” shall be 30 working days.
<b>10.7</b>	NOT USED
<b>10.8</b>	<b>Protection of Customer Data</b> (Clause 35.2.3 of the Call Off Terms):

10.9	<p><b>Notices</b> (Clause 56.6 of the Call Off Terms):</p> <p>Customer's postal address and email address:</p> <p>Mutual Ventures Limited 2-6 Boundary Row London SE1 8HP</p> <p>Supplier's postal address and email address:</p> <p>David Fairhurst Mutual Ventures Limited 2-6 Boundary Row London SE1 8HP</p>
10.10	<p><b>Transparency Reports</b></p> <p>In Call Off Schedule 13 (Transparency Reports)</p>
10.11	<p><b>Alternative and/or additional provisions (including any Alternative and/or Additional Clauses under Call Off Schedule 14 and if required, any Customer alternative pricing mechanism):</b></p> <p>Not applicable</p>
10.12	<p><b>Call Off Tender:</b></p> <p>In Call Off Schedule 16</p>
10.13	<p><b>Publicity and Branding (Clause 36.3.2 of the Call Off Terms)</b></p> <p>Not applicable</p>
10.14	<p><b>Staff Transfer</b></p> <p>Annex to Call Off Schedule 10, List of Notified Sub-Contractors (Call Off Tender).</p>

10.15

**Processing Data**

Call Off Schedule 17.

Please also see Annex D for GDPR clauses.

1. The contact details of the Customer Data Protection Officer is:  
  
Emma Wharram  
Departmental Data Protection Officer, BRISTOL - 2 RIVERGATE
2. The contact details of the Suppliers Data Protection Officer is:  
  
David Fairhurst  
Mutual Ventures Limited, 2-6 Boundary Row, London, SE1 8HP
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
4. Any such further instructions shall be incorporated into this Schedule.

<b>Contract Reference:</b>	
<b>Date:</b>	<b>2 March 2020</b>
<b>Description Of Authorized Processing</b>	<b>Details</b>
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation the Parties are independent controllers of Personal Data under this Framework Agreement.
Use of Personal Data	Managing the obligations under the Call Off Contract Agreement, including exit management, and other associated activities.

	Duration of the processing	For the duration of the Framework Award plus 7 years.
	Nature and purposes of the processing	The Supplier will need access to the names, job titles and workplace email addresses of the Local Authorities in the Strengthening Families, Protecting Children Programme, in order to make contact and carry out their work as stipulated in the Contract.
	Type of Personal Data	<ul style="list-style-type: none"> <li>• Full name</li> <li>• Workplace email address</li> <li>• Job Title</li> </ul>
	Categories of Data Subject	Staff of the Local Authorities in the Strengthening Families, Protecting Children Programme.
<b>10.16</b>	<b>MOD DEFCONs and DEFFORM</b>	
	Call Off Schedule 15	

## FORMATION OF CALL OFF CONTRACT

**BY SIGNING AND RETURNING THIS CALL OFF ORDER FORM (which may be done by electronic means) the Supplier agrees to enter a Call Off Contract with the Customer to provide the Services in accordance with the terms Call Off Order Form and the Call Off Terms.**

**The Parties hereby acknowledge and agree that they have read the Call Off Order Form and the Call Off Terms and by signing below agree to be bound by this Call Off Contract.**

**In accordance with paragraph 7 of Framework Schedule 5 (Call Off Procedure), the Parties hereby acknowledge and agree that this Call Off Contract shall be formed when the Customer acknowledges (which may be done by electronic means) the receipt of the signed copy of the Call Off Order Form from the Supplier within two (2) Working Days from such receipt.**

For and on behalf of the Supplier:		For and on behalf of the Customer:	
Signature:	 David Fairhurst (Apr 22, 2020)	Signature:	 Stephanie Brivio (Apr 22, 2020)
Name:	David Fairhurst	Name:	Stephanie Brivio
Role:	Executive Chair	Role:	Deputy Diector, C
Date:	Apr 22, 2020	Date:	Apr 22, 2020



## Annex A – Initial Delivery Plan and KPIs

### Support plan until July 2020

The unprecedented COVID19 crisis has led to rapid and significant changes in the focus and workload of the local authority teams involved in the Strengthening Families Programme; and of course across England. This work has quite rightly been absorbing senior and frontline children's services teams who are adopters on the programme.

We are confident, however, that we can and should continue to work with the innovators during the pause in work with adopters. **The 'pause' provides a useful opportunity to develop tools, methods, relationships and an understanding of the new context that will enhance the impact of future work.**

**Perhaps most importantly, the innovators themselves are ready, keen and have capacity to get going with this work straightaway.**

Over the last 12 months the innovators have been working with three trailblazers. They have, in innovation terminology, been 'prototyping' their approach to scaling. It is good practice to create space to learn from and build on that work before moving into the next phase of delivery. The work with adopter sites, once it restarts, can only be richer as a result. Further:

- **We have identified a range of valuable work that we can do together with the innovator sites in the next four months.** They are keen to do this work and have capacity to do it, despite COVID19 (their scaling teams are separate from mainstream LA structures). We expect there to be more work once we have engaged further with the innovators.
- **We can develop the working partnerships between our coaches, the innovator teams and our DfE colleagues** so that we all move into the new work with the adopter sites as a well-developed partnership - having moved through the 'forming, norming and storming' phases of team building before we re-engage.
- **We can begin the design of the wider learning programme** that will focus on adopters and the wider sector so it is ready to roll out once the adopter work restarts.
- **We can support the innovators to design a post-Covid-19 diagnostic to use when we all re-engage with the sites.** Much will have changed for each adopter due to COVID19 on the ground and each locality will be recovering from an intense period of unprecedented work. Understanding what has changed for them will be crucial to getting the adoption work right in the future. We have described a live learning process we can use.
- **We can support the innovators to design and prototype post-Covid-19 adaptations to their innovations** where appropriate - to ensure that their own work and the work they are doing with adopters is of the highest relevance and impact.
- **We can hold our best delivery teams in place if we continue to work with the innovators through the pause,** and ensure they are ready to work with the adopters in 4 months time. We have outlined this in more detail below.

More detail around the work and a high level plan are below.

### **We have identified valuable work with the innovator sites that can commence now**

We have now spoken to each of the innovator sites and our assessment is that there is valuable work that we can do together over the next four months that will set them up to re-engage with sites. They are keen to get moving on this work, and excited that we have been engaged and will bring skills and expertise that they value.

With all three innovators we think that we can productively use this time to:

- Understand and assess how they have been delivering site support over the past 12 months and help them identify what has been working and what has been less successful.
- Connect them with each other to share that learning so that their future site support draws on their collective experience (they are keen to meet as a group and have not done so to date)
- Support them to refine their approaches to working with the future adopters, including co-designing how the coach and innovator roles will work
- Develop highly impactful materials and tools that will enhance their ability to work later in the year
- Upskill their teams in some key skills that team leads feel are currently lacking

We need to have a fuller discovery session with each innovator and our teams to co-design this work together, and would expect there to be more that will emerge. But based on our early conversations the scope is as follows.

### Hertfordshire

- Test the approach they have been using with their trailblazer site, think through what they have learned and what could/should change as they move forward
- Design how a community of practice would work, how to connect it to the current practice community that exists around Family Safeguarding
- Re-design and support the further development of materials to use with sites - the team are skilled practitioners but not experienced in writing and visual comms
- Get all of the materials into really good shape, this could include the development of a handbook similar to the one that exists now for NYCC, slides, training materials etc
- Public speaking and training design support for the team - they lack confidence around public speaking and delivery
- Training in running remote workshops - we have two solutions using both Zoom and Microsoft Teams and could coach the teams in how to run effective virtual workshops
- Refine the cost / benefit analysis tool to suit the new sites

### Leeds

- Test the approach they have been using with their trailblazer site, think through what they have learned and what could/should change as they move forward (e.g. examine and enhance the change management approach to effective implementation of relational practice)
- Re-design and support the further development of materials to use with sites - the team are skilled practitioners but not experienced in written and visual communications for innovation adoption
- Support the design of new materials and content to support the implementation of Family Valued, this could include a handbook similar to the one that exists now for NYCC
- Support the development of their new website, materials and content to support the implementation of FV including a webinar capability so that they can offer online tuition to participating authorities

### NYCC

- Test the approach they have been using with their trailblazer site, think through what they have learned and what could/should change as they move forward
- Revise the materials that they have been using with Middlesbrough and refine them with the team to make them more impactful
- Help them to think differently about online learning and tools that could support them to work with sites in different ways
- If need be, provide some more direct capacity into the NYCC team as we know both the team and the model well through leading its adoption into GM

### Learning work

There are some key things that we can do around learning in the next four months.

*Develop a shared understanding of what it takes to successfully scale innovation in children's social care.*

This would combine their learning to date, with our deep understanding of the literature and practice in other sectors. Therefore, we will:

- Bring all three teams together to connect with each other and facilitate structured learning sessions on their experiences of scaling.
- Share evidence from the literature and from our own experience in this and other sectors - from the wider GM work to adopt NWD, and the scaling of a large, community based mental health innovation that Innovation Unit is leading across the UK (Siobhan Edwards also works on this programme).
- Co-develop a framework to capture and share this learning. This will help discipline their work - with the support of their coaches - with new adopters. It will also be a product that we can share more widely with the sector.

*Co-design the learning programme with them.*

We would work in partnership with innovators, the DfE team and the WWC to understand objectives, scope and parameters - and to build on what has worked well to date. We could begin to produce materials. The timings will need to wait until we are closer to re-engaging with the sites.

*Build a diagnostic for re-engaging with the sites using live learning within the innovator sites.*

We expect that all children's teams across the country will come out the other side of COVID19 in very different places to where they are now. For the adopter sites, we need to understand the magnitude of that change and how this will impact on the future programme. We propose to do this via live learning with the innovator sites - using learning tools to support them to understand what has been changing as a result of COVID for them, and what it takes to be successful with their innovations in this new environment. We know the innovators are high performing authorities so this will not directly map across, but it is a good place to start in terms of understanding the changing context. This will enable us to support the innovators to build a revised diagnostic that we can jointly conduct with the sites once we are able to re-engage.

*Support the innovators to design and prototype post-Covid-19 adaptations to their innovations*

As above, there may be adaptations to the innovations themselves that are necessary to ensure that their own work and the work they are doing with adopters is of the highest relevance and impact. We would support the innovators to do this work quickly and rigorously, producing learning materials for adopters as they go.

### **The work can be delivered despite COVID19**

We feel confident that we can deliver this work with the innovators for a number of reasons.

The innovators have the capacity to keep working on the programme. They all have separate teams that are focused on Strengthening Families:

- Sue Williams from Hertfordshire and Steve Walker from Leeds and their teams are not directly involved in the COVID work in their LA - they need to use this time productively and we can help
- Janice Nicholson was drawn into COVID19 planning in the last few weeks, although her team was not. She has re-engaged now, but going forward should she need to focus elsewhere, we know she is well supported by Sarah Walston and David Gillson who are extremely capable, and we could step in to support them more directly

They have all expressed their pleasure at our appointment and their keenness to start work with us as soon as possible.

The work we have identified can be delivered remotely. All of the work we have outlined in this document is well suited to remote work, which our teams are increasingly adept with. We have online tools we can use to work in different ways with each other - our teams have all been reimagining how to use these tools over the last 10 days. It is possible that we will not need to socially distance for the whole of the four months so it might be possible to meet in smaller groups, additionally, over time.

You also know the flexibility and quality of our work. In our work on the CSC Innovation Programme we have demonstrated our ability to flex to meet the needs of the work, under pressure. We would propose that you allow us to start this work and we revisit things in two months to test the progress we are making.

**Proposed plan**

We have proposed below a high level plan for how we would take this work forward.

<REDACTED>

**Key performance indicators during SFPC programme delivery**

Service area	What outcomes do we want from the project support provider?	How do we propose to measure their success?	Frequency of measurement	Method of measurement	Target
Project implementation and change management support	<ul style="list-style-type: none"> <li>Each adopter LA (the authorities who will take part in the programme to adapt and adopt their chosen model in their area) and innovator LA (Leeds, Hertfordshire and North Yorkshire) receives high-quality, tailored support to successfully implement their projects. This includes advice on the following areas: <ul style="list-style-type: none"> <li>Project planning, management and governance;</li> <li>Business planning and financial modelling to support the future sustainability of their model;</li> <li>Mobilisation and capacity building;</li> <li>Recruitment and resourcing;</li> <li>Stakeholder management and networking.</li> </ul> </li> <li>High quality, tailored implementation plans are put in place for each project</li> <li>Each adopter and innovator LA are supported and held to account for delivering against their implementation plans</li> </ul>	<p>We propose to monitor and measure this service area against the following indicators during the monthly contract management meetings and/or formal six month contract reviews:</p> <ul style="list-style-type: none"> <li>The timeliness in which implementation plans are agreed and updated for each project;</li> <li>The number and frequency of days given to support each project;</li> <li>The number of projects rated as 'good' or better across their 'score card' r (score card and definition of 'good' etc. to be agreed between the Department for Education (DfE) and chosen provider)</li> <li>Anonymous feedback from project participants on their experience of the quality of support given to them (content of questionnaire to be agreed between the DfE and chosen provider, but likely to include indicators on: accessibility of support, their effectiveness of delivering solutions to problems, quality of advice and technical expertise, level of constructive challenge, leadership development)</li> </ul>	<p>Monthly</p> <p>Quarterly report (to include scorecard)</p> <p>Questionnaire developed every six months, starting from month 6 (August 2020)</p>	<p>Reports on time spent on projects and progress with implementation in monthly update meetings between MV core team and DFE</p> <p>Detailed review in quarterly reports (to include scorecard)</p> <p>Anonymised feedback from project participants and the DFE team on their experience of the coaching support using a questionnaire to be developed and agreed with the DFE.</p>	<p>Project implementation plans to be agreed by end of month 2.</p> <p>Number of days to be delivered in line with individual requirements of each LA, and reported to DFE at monthly update meetings.</p> <p>65% good or above on score card. Good: 'Project on track against programme plan and all risks mapped with clear mitigating actions.'</p> <p>Feedback on questionnaire to be 75% or above positive response</p>
Supporting effective working relationships	<ul style="list-style-type: none"> <li>High-quality, impartial advice and mediation support is given between the innovator LAs, adopter LAs and their local partners, especially when working relationship dynamics are challenging</li> <li>Innovator LAs and adopter LAs report that their working relationship dynamics improve following the advice and intervention from the project support provider</li> </ul>	<p>We propose to monitor and measure this service area against the following indicators during the monthly contract management meetings and/or formal six month contract reviews:</p> <ul style="list-style-type: none"> <li>See KPI above on anonymous feedback from project participants (questionnaire to include an indicator on the quality of mediation support and effectiveness of intervention from the project support provider when working relationships are challenging)</li> </ul>	<p>See previous response on bi annual questionnaire. Questionnaire will be drafted to gather responses on all relevant issues.</p>	<p>Anonymised feedback from project participants and the DFE team on their experience of the coaching support using a questionnaire to be developed and agreed with the DFE.</p>	<p>75% or above positive responses</p>
Spreading of learning	<ul style="list-style-type: none"> <li>The project support provider facilitates the effective spreading of</li> </ul>	<p>We propose to monitor and measure this service area against the following indicators during the</p>	<p>Monthly and six monthly</p>	<p>Learning programme to be developed and shared with DFE.</p>	<p>Learning Programme to be developed and shared with DFE by</p>

	<p>learning from the programme across adopter LAs and innovator LAs.</p> <ul style="list-style-type: none"> <li>• The project support provider facilitates the effective spreading of learning from the programme to the wider sector.</li> <li>• Adopter LAs, innovator LAs and the wider sector accesses and benefits from the findings.</li> </ul>	<p>monthly contract management meetings and/or formal six month contract reviews:</p> <ul style="list-style-type: none"> <li>• The number and frequency of learning materials (events or tools etc.) produced by the project support provider to share learning across the adopter and innovator LAs and, importantly, with the wider sector.</li> <li>• The number of people and LAs accessing these learning materials (i.e. numbers attending events, numbers of downloads/material usage etc.)</li> <li>• Anonymous feedback from users shows that the learning materials that have been produced are high quality.</li> </ul>		<p>Data on each learning event to be captured through standardised form developed by the Learning Director (attendees, material usage) and reported to DFE</p> <p>Short surveys to be issued after each event, to inform planning for the next.</p>	<p>end of month 2, with events scheduled by end of month 3</p> <p><b>Attendance and usage targets to be updated following development of the Learning Programme</b></p> <p>80% positive feedback from event attendees in surveys</p>
Project monitoring	<ul style="list-style-type: none"> <li>• The Department for Education (DfE) receives regular, timely and accurate insights into the progress of individual projects and the programme as a whole.</li> <li>• Any issues/barriers to delivery within individual projects are identified and addressed in a timely manner, to ensure that each project progresses as effectively as possible.</li> <li>• Any wider barriers to delivery or common issues across multiple projects are identified and reported to DfE in a timely manner. High quality solutions are proposed and implemented to address any these.</li> </ul>	<p>We propose to monitor and measure this service area against the following indicators during the monthly contract management meetings and/or formal six month contract reviews:</p> <ul style="list-style-type: none"> <li>• The frequency and timeliness of status reports submitted to the DfE on individual projects and the programme as a whole.</li> <li>• The quality of information given in the status reports, including proposed solutions to addressing any wider barriers to delivery/common issues across multiple projects.</li> </ul>	<p>Quarterly monitoring through written reports</p> <p>Monthly monitoring through face to face meetings</p>	<p>Quarterly reports on status to be submitted to the DFE quarterly.</p> <p>DFE to be informed of status updates at monthly progress review meetings.</p> <p>Any exceptional issues to be reported to the DFE as they arise.</p>	<p><b>95%</b> quarterly reports to be submitted on time to DFE in accordance with project plan. Exceptions to be clearly communicated to DFE ahead of time.</p> <p>Positive feedback from DFE on information given in status reports.</p>

**Annex B – Forecast and payment profile**

<REDACTED>

## Annex C – DfE Security Policy

### Departmental Security standards for Business Services and ICT contracts

<p>“BPSS” “Baseline Personnel Security Standard”</p>	<p>means the Government’s HMG Baseline Personal Security Standard . Further information can be found at: <a href="https://www.gov.uk/government/publications/government-baseline-personnel-security-standard">https://www.gov.uk/government/publications/government-baseline-personnel-security-standard</a></p>
<p>“CCSC” “Certified Cyber Security Consultancy”</p>	<p>is the National Cyber Security Centre’s (NCSC) approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. See website: <a href="https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy">https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy</a></p>
<p>“CCP” “Certified Professional”</p>	<p>is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession. See website: <a href="https://www.ncsc.gov.uk/information/about-certified-professional-scheme">https://www.ncsc.gov.uk/information/about-certified-professional-scheme</a></p>
<p>“CPA” “Commercial Product Assurance” [formerly called “CESG Product Assurance”]</p>	<p>is an ‘information assurance scheme’ which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards.. See website: <a href="https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa">https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa</a></p>
<p>“Cyber Essentials” “Cyber Essentials Plus”</p>	<p>Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme. There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to these providers: <a href="https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body">https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body</a></p>
<p>“Data” “Data Controller” “Data Protection Officer” “Data Processor” “Personal Data” “Personal Data requiring Sensitive Processing”</p>	<p>shall have the meanings given to those terms by the Data Protection Act 2018</p>

<p>“Data Subject”, “Process” and “Processing”</p>	
<p>“Department’s Data” “Department’s Information”</p>	<p>is any data or information owned or retained in order to meet departmental business objectives and tasks, including: (a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are:     (i) supplied to the Contractor by or on behalf of the Department; or     (ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or (b) any Personal Data for which the Department is the Data Controller;</p>
<p>“DfE” “Department”</p>	<p>means the Department for Education</p>
<p>“Departmental Security Standards”</p>	<p>means the Department’s security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver.</p>
<p>“Digital Marketplace / G-Cloud”</p>	<p>means the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects.</p>
<p>End User Devices</p>	<p>means the personal computer or consumer devices that store or process information.</p>
<p>“Good Industry Practice” “Industry Good Practice”</p>	<p>means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.</p>
<p>“Good Industry Standard” “Industry Good Standard”</p>	<p>means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.</p>

<p>“GSC” “GSCP”</p>	<p>means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: <a href="https://www.gov.uk/government/publications/government-security-classifications">https://www.gov.uk/government/publications/government-security-classifications</a></p>
<p>“HMG”</p>	<p>means Her Majesty’s Government</p>
<p>“ICT”</p>	<p>means Information and Communications Technology (ICT) and is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution</p>
<p>“ISO/IEC 27001” “ISO 27001”</p>	<p>is the International Standard for Information Security Management Systems Requirements</p>
<p>“ISO/IEC 27002” “ISO 27002”</p>	<p>is the International Standard describing the Code of Practice for Information Security Controls.</p>
<p>“ISO 22301”</p>	<p>is the International Standard describing for Business Continuity</p>
<p>“IT Security Health Check (ITSHC)” “IT Health Check (ITHC)” “Penetration Testing”</p>	<p>means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.</p>
<p>“Need-to-Know”</p>	<p>means the Need-to-Know principle employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties.</p>
<p>“NCSC”</p>	<p>The National Cyber Security Centre (NCSC) is the UK government’s National Technical Authority for Information Assurance. The NCSC website is <a href="https://www.ncsc.gov.uk">https://www.ncsc.gov.uk</a></p>
<p>“OFFICIAL” “OFFICIAL-SENSITIVE”</p>	<p>the term ‘OFFICIAL’ is used to describe the baseline level of ‘security classification’ described within the Government Security Classification Policy (GSCP).</p> <p>the term ‘OFFICIAL–SENSITIVE is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the GSCP.</p>
<p>“RBAC” “Role Based Access Control”</p>	<p>means Role Based Access Control. A method of restricting a person’s or process’ access to information depending on the role or functions assigned to them.</p>

<p>“Storage Area Network” “SAN”</p>	<p>means an information storage system typically presenting block based storage (i.e. disks or virtual disks) over a network interface rather than using physically connected storage.</p>
<p>“Secure Sanitisation”</p>	<p>means the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level.</p> <p>NCSC Guidance can be found at: <a href="https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media">https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media</a></p> <p>The disposal of physical documents and hardcopy materials advice can be found at: <a href="https://www.cpni.gov.uk/secure-destruction">https://www.cpni.gov.uk/secure-destruction</a></p>
<p>“Security and Information Risk Advisor” “CCP SIRA” “SIRA”</p>	<p>means the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also: <a href="https://www.ncsc.gov.uk/articles/about-certified-professional-scheme">https://www.ncsc.gov.uk/articles/about-certified-professional-scheme</a></p>
<p>“Senior Information Risk Owner” “SIRO”</p>	<p>means the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for overseeing the management of information risk across the organisation. This includes its executive agencies, arms length bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties.</p>
<p>“SPF” “HMG Security Policy Framework”</p>	<p>means the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government’s Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. <a href="https://www.gov.uk/government/publications/security-policy-framework">https://www.gov.uk/government/publications/security-policy-framework</a></p>

- 12.1. The Contractor shall be aware of and comply the relevant [HMG security policy framework](#), [NCSC guidelines](#) and where applicable DfE Departmental Security Standards for Contractors which include but are not constrained to the following clauses.
- 12.2. Where the Contractor will provide products or services or otherwise handle information at OFFICIAL for the Department, the requirements of [Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - Action Note 09/14](#) dated 25 May 2016, or any subsequent updated document, are mandated; that “contractors supplying products or services to HMG shall have achieved, and will be expected to retain certification at the appropriate level for the duration of the contract. The certification scope shall be relevant to the services supplied to, or on behalf of, the Department.
- 12.3. Where clause 12.2 above has not been met, the Contractor shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements).
- The ISO/IEC 27001 certification must have a scope relevant to the services supplied to, or on behalf of, the Department. The scope of certification and the statement of applicability must be acceptable, following review, to the Department, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).
- 12.4. The Contractor shall follow the UK Government Security Classification Policy (GSCP) in respect of any Departmental Data being handled in the course of providing this service and will handle all data in accordance with its security classification. (In the event where the Contractor has an existing Protective Marking Scheme then the Contractor may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Departmental Data).
- 12.5. Departmental Data being handled in the course of providing an ICT solution or service must be separated from all other data on the Contractor’s or sub-contractor’s own IT equipment to protect the Departmental Data and enable the data to be identified and securely deleted when required in line with clause 12.14.

- 12.6 The Contractor shall have in place and maintain physical security to premises and sensitive areas in line with ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access), CCTV, alarm systems, etc.
- 12.7 The Contractor shall have in place and maintain an appropriate user access control policy for all ICT systems to ensure only authorised personnel have access to Departmental Data. This policy should include appropriate segregation of duties and if applicable role based access controls (RBAC).
- 12.8 The Contractor shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to:
- physical security controls;
  - good industry standard policies and processes;
  - malware protection;
  - boundary access controls including firewalls;
  - maintenance and use of fully supported software packages in accordance with vendor recommendations;
  - software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;
  - user access controls, and;
  - the creation and retention of audit logs of system, application and security events.
- 12.9 The contractor shall ensure that any departmental data (including email) transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.
- 12.10 The contractor shall ensure that any departmental data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the department except where the department has given its prior written consent to an alternative arrangement.
- 12.11 The contractor shall ensure that any device which is used to process departmental data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/end-user-device-security> and <https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles>.
- 12.12 Whilst in the Contractor's care all removable media and hardcopy paper documents containing Departmental Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.

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

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

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

12.14 In the event of termination of contract due to expiry, liquidation or non-performance, all information assets provided, created or resulting from the service shall not be considered as the supplier's assets and must be returned to the department and written assurance obtained from an appropriate officer of the supplying organisation that these assets regardless of location and format have been fully sanitised throughout the organisation in line with clause 12.15.

- 12.15 In the event of termination, equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored by the Contractor must be accounted for and either physically returned or securely sanitised or destroyed in accordance with the current HMG policy using an NCSC approved product or method.

Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as data stored in a cloud system, Storage Area Network (SAN) or on shared backup tapes, then the Contractor or sub-contractor shall protect the Department's information and data until such time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.

Evidence of secure destruction will be required in all cases.

- 12.16 Access by Contractor or sub-contractor staff to Departmental Data shall be confined to those individuals who have a "need-to-know" in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Department. All Contractor or sub-contractor staff must complete this process before access to Departmental Data is permitted.
- 12.17 All Contractor or sub-contractor employees who handle Departmental Data shall have annual awareness training in protecting information.
- 12.18 The Contractor shall, as a minimum, have in place robust Business Continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the services delivered. If a ISO 22301 certificate is not available the supplier will provide evidence of the effectiveness of their ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures. This should include evidence that the Contractor has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.
- 12.19 Any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data handled in the course of providing this service shall be recorded as an incident. This includes any non-compliance with these Departmental Security Standards for Contractors, or other Security Standards pertaining to the solution.

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

Incidents shall be reported through the department's nominated system or service owner.

Incidents shall be investigated by the contractor with outcomes being notified to the Department.

- 12.20 The Contractor shall ensure that any IT systems and hosting environments that are used to handle, store or process Departmental Data shall be subject to independent IT Health Checks (ITHC) using an NCSC CHECK Scheme ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Department and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.
- 12.21 The Contractor or sub-contractors providing the service will provide the Department with full details of any actual or future intent to develop, manage, support, process or store Departmental Data outside of the UK mainland. The Contractor or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Department.
- 12.22 The Department reserves the right to audit the Contractor or sub-contractors providing the service within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being supplied and the Contractor's, and any sub-contractors', compliance with the clauses contained in this Section.
- 12.23 The Contractor and sub-contractors shall undergo appropriate security assurance activities and shall provide appropriate evidence including the production of the necessary security documentation as determined by the department. This will include obtaining any necessary professional security resources required to support the Contractor's and sub-contractor's security assurance activities such as: a Security and Information Risk Advisor (SIRA) certified to NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Cyber Professional (CCP) schemes.
- 12.24 Where the Contractor is delivering an ICT solution to the Department they shall design and deliver solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current NCSC Information Assurance Guidance and Departmental Policy. The Contractor will provide the Department with evidence of compliance for the solutions and services to be delivered. The Department's expectation is that the Contractor shall provide written evidence of:
- Compliance with HMG Minimum Cyber Security Standard.
  - Any existing security assurance for the services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification.
  - Any existing HMG security accreditations or assurance that are still valid including: details of the awarding body; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement.
  - Documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Contractor shall provide details of who the awarding body or organisation will be and date expected.
- 12.25 The Contractor shall contractually enforce all these Departmental Security Standards for Contractors onto any third-party suppliers, sub-contractors or partners who could potentially access Departmental Data in the course of providing this service.

## Annex D – GDPR clauses

### General Data Protection Regulation (GDPR)

“Controller”, “Processor,” “Data Subject”, “Personal Data”, “Personal Data Breach”, “Data Protection Officer”	take the meaning given in the GDPR
“Data Loss Event”	any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach.
“DPA 2018”	Data Protection Act 2018
“Data Protection Impact Assessment”	an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.
“Data Protection Legislation”	(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 [subject to Royal Assent] 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 Request”	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.
“GDPR”	the General Data Protection Regulation (Regulation (EU) 2016/679)
“Joint Controllers”	Where two or more Controllers jointly determine the purposes and means of processing
“Law”	means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Processor is bound to comply;

“LED”	Law Enforcement Directive (Directive (EU) 2016/680)
“Processor Personnel”	employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Contract.
“Protective Measures”	appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those set out in the Contract.
“Sub-processor”	any third Party appointed to process Personal Data on behalf of the Processor related to this Contract

## **17 Data Protection**

- 17.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor unless otherwise specified in Schedule 3a. The only processing that the Processor is authorised to do is listed in Schedule 3a by the Controller and may not be determined by the Processor
- 17.2 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.
- 17.3 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:
- (a) a systematic description of the envisaged processing operations and the purpose of the processing;
  - (b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;
  - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
  - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
- 17.4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Contract:
- (a) process that Personal Data only in accordance with Schedule 3a , unless the Processor is required to do otherwise by Law. If it is so required the Processor shall

promptly notify the Controller before processing the Personal Data unless prohibited by Law;

- (b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:
  - (i) nature of the data to be protected;
  - (ii) harm that might result from a Data Loss Event;
  - (iii) state of technological development; and
  - (iv) cost of implementing any measures;
  
- (c) ensure that:
  - (i) the Processor Personnel do not process Personal Data except in accordance with this Contract (and in particular Schedule 3a);
  - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
    - (A) are aware of and comply with the Processor's duties under this clause;
    - (B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
    - (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Contract; and
    - (D) have undergone adequate training in the use, care, protection and handling of Personal Data; and
  
- (d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
  - (i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;
  - (ii) the Data Subject has enforceable rights and effective legal remedies;
  - (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
  - (iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

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

17.5 Subject to clause 17.6, the Processor shall notify the Controller immediately if it:

- (a) receives a Data Subject Request (or purported Data Subject Request);
- (b) receives a request to rectify, block or erase any Personal Data;
- (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
- (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;
- (e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
- (f) becomes aware of a Data Loss Event.

17.6 The Processor's obligation to notify under clause 17.5 shall include the provision of further information to the Controller in phases, as details become available.

17.7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 17.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

- (a) the Controller with full details and copies of the complaint, communication or request;
- (b) such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;
- (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
- (d) assistance as requested by the Controller following any Data Loss Event;
- (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

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

- (a) the Controller determines that the processing is not occasional;
- (b) the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
- (c) the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

- 17.9 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
- 17.10 Each Party shall designate its own data protection officer if required by the Data Protection Legislation.
- 17.11 Before allowing any Sub-processor to process any Personal Data related to this Contract, the Processor must:
- (a) notify the Controller in writing of the intended Sub-processor and processing;
  - (b) obtain the written consent of the Controller;
  - (c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause 17 such that they apply to the Sub-processor; and
  - (d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.
- 17.12 The Processor shall remain fully liable for all acts or omissions of any Sub-processor.
- 17.13 The Controller may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Contract).
- 17.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

### **Schedule 3a Processing, Personal Data and Data Subjects**

Refer to paragraph 10.15 of the Call Off Order Form.

## **ANNEX E - Customer Project Specification**

### **Strengthening Families, Protecting Children Programme Project Support Provider Specification**

#### **Contract specification summary**

The Department for Education is looking to tender a contract to an external organisation to provide high-quality, tailored support and expertise to local authorities involved in the Children's Social Care *Strengthening Families, Protecting Children* programme, to support the successful implementation of whole-system change to the way children's social care services are delivered in up to 20 councils.

#### **Background to the *Strengthening Families, Protecting Children* programme**

The Autumn Budget 2018 made available up to £84m over five years for the Children's Social Care *Strengthening Families, Protecting Children* (SFPC) programme.

The purpose of this programme is to support up to 20 local authorities with high or rising demand for children's social care services to improve the support they offer to vulnerable children and their families. Through this, the programme aims to enable more children to stay at home thriving in stable family environments where it is safe for them to do so, and safely reduce the number of children entering care.

The programme will do this by investing up to £84m over five years from April 2019 to support local authorities to adapt and adopt one of three projects developed by Leeds, Hertfordshire, or North Yorkshire. These three projects were funded in Round One of the Department for Education's Children's Social Care Innovation Programme. This programme, launched in 2014, looked to support innovative ideas to flourish, and better enable policy and practice to be driven by a strong evidence base of what works. All projects were independently evaluated. The three chosen projects for the SFPC programme (Leeds 'Family Valued', Hertfordshire 'Family Safeguarding', and North Yorkshire's 'No Wrong Door') all demonstrated the most promising evidence of safely managing demand at the more severe end of the children's social care spectrum.

#### **Programme delivery**

The SFPC programme was formally launched in April 2019, along with the announcement of the criteria of which local authorities are eligible to take part. Over the spring and summer, the department has worked to identify which of these eligible authorities will take part in the programme as 'adopter' LAs, based on a rigorous assessment of their need, commitment and suitability.

From Autumn 2019, the adopter local authorities will come onto the programme in a staggered way – roughly, we expect between 1 to 3 adopter LAs to start work every 6 months. They will work to implement either the Leeds, Hertfordshire or North Yorkshire model, and will receive intensive implementation support from their corresponding 'innovator' LA (who developed their chosen model) to do this.

In order to support this delivery and ensure successful implementation, the department is looking to commission an external project support provider to provide high-quality support, guidance and challenge to both adopter and innovator LAs.

#### **Contract specification**

Implementing their chosen model will be a complex process for all adopter LAs. Each model requires a system-wide change to the way their services work, involving changes to processes, systems, staffing structures, and - most critically and most challengingly - culture and ethos.

While the expertise of their corresponding innovator LA (Leeds, Hertfordshire or North Yorkshire) will be central to managing this change, we are looking for a further layer of expert support, advice and challenge to be provided by a project support provider.

Further detail on the services that a project support provider will be expected to provide is outlined below, but the successful bidding organisations will be able to demonstrate that they have skills and expertise to provide these. Although not exhaustive, the main skills and expertise required include:

- detailed knowledge and understanding of the social care sector, preferably with a particular focus on children's social care;
- expertise in how to manage and maintain momentum of change across large and complex organisations, particularly how to shift culture and practice, including across partner organisations;
- experience and credibility when working with and influencing a wide range of senior stakeholders across children's social care, local government, health, police, and central government;
- access to a range of technical expertise, including legal, HR, procurement, finance and investment, governance, stakeholder management, capturing and codifying learning, business planning and sustainability, and impact measurement and cost-benefit analysis; and,
- understanding of how to facilitate the sharing of learning and best practice, both between projects and across the wider children's social care sector.

While we will work closely with the successful bidder to design the specifics of a programme of work, there are four main areas that we expect a project support provider to provide support with: project implementation and change management; project monitoring; coaching and supporting effective working relationships; and spreading of learning to the sector. More detail on each of these areas is provided below.

Support should be proportionate to the needs of projects, which may fluctuate or decrease over the lifetime of the Department's funding. This means there needs to be an ongoing review of processes to inform any adjustment of the support model.

#### **A. Project implementation and change management support**

We are looking for a project support provider to use their expertise in project implementation and change management to provide support and challenge to each adopter LA (the authorities who will take part in the programme to adapt and adopt their chosen model in their area) and their corresponding innovator LA (who developed their chosen model) to ensure their projects are delivered successfully.

We expect each adopter LA to work flexibly with their chosen model, and - in close partnership with their innovator LA - design an approach to implementation that is bespoke to their context and existing strengths. As such, the support they receive from the project support provider should be tailored, flexible, and responsive to how the needs of the LAs change over the course of the programme.

Projects particularly value advice, support and challenge from experts who are independent from the Department, and are able to give high quality, technical support, including on the following areas:

- project mobilisation and maintaining momentum of change;
- recruitment, resourcing and capacity building;
- brokering relationships;
- project planning and management;
- project governance;

- stakeholder management and networking; and
- sustainability and business planning.

## **B. Supporting effective working relationships**

Successful implementation of these projects will require effective working between several key partners. As well as the close partnership between adopter and innovator LAs, the programme will also require a good working relationships with 'What Works for Children's Social Care' (WWC) who are leading the evaluation of the SFPC programme.

The project support provider will provide high-quality, impartial advice and have the coaching and mediation skills to support these relationships to flourish, including when dynamics between partners are challenging.

## **C. Spreading of learning**

The SFPC programme will be fully evaluated by WWC, but this comprehensive outcomes-based evaluation will be long-term and it will not be finalised until 2024. In the meantime, we want a 'live learning system' to be developed to support action learning between participating adopter LAs, innovator LAs, and, importantly, outwards to the wider sector.

The project support provider will be expected to work closely with WWC, DfE and innovator LAs to design and deliver a high-quality action learning strategy to facilitate the effect sharing of learning from the programme and to support with the capture, codification and sharing of learning across the system.

## **D. Project monitoring**

The Department is looking for an organisation to offer regular, timely and accurate external insights into the progress of projects and identify barriers to delivery. This insight will ensure the right support is given to projects, build a wider understanding of common challenges faced by multiple projects and spread evidence-based practice.

Projects will report quarterly on progress, spend, challenges faced and issues moving forward, as part of the Department's efforts to support and monitor the delivery and impact of projects. The successful project support provider would feed into these reports, offering their insight on project progress and sustainability.

The support provider would also work closely with the Department to design and deliver high-quality solutions to address the issues faced by projects in a timely manner.

### **Performance indicators**

The indicators that we currently propose to monitor and measure the chosen project support provider against are listed below. However, please note that these KPIs are indicative and will be developed, refined and agreed between the appointed project support provider and the DfE.

We would expect to monitor these indicators during monthly contract management meetings and/or formal six-month contract reviews.

### **Project implementation and change management support**

We propose to monitor and measure this service area against the following indicators:

- The timeliness in which implementation plans are agreed and updated for each project;
- The number and frequency of days given to support each project;

- The number of projects rated as 'good' or better across their 'score card' (score card and definition of 'good' etc. to be agreed between the DfE and chosen provider)
- Anonymous feedback from project participants on their experience of the quality of support given to them (content of questionnaire to be agreed between the DfE and chosen provider, but likely to include indicators on: accessibility of support, their effectiveness of delivering solutions to problems, quality of advice and technical expertise, level of constructive challenge, leadership development)

### **Supporting effective working relationships**

We propose to monitor and measure this service area against the following indicators:

- See KPI above on anonymous feedback from project participants (questionnaire to include an indicator on the quality of mediation support and effectiveness of intervention from the project support provider when working relationships are challenging)

### **Spreading of learning**

We propose to monitor and measure this service area against the following indicators:

- The number and frequency of learning materials (events or tools etc.) produced by the project support provider to share learning across the adopter and innovator LAs and, importantly, with the wider sector.
- The number of people and LAs accessing these learning materials (i.e. numbers attending events, numbers of downloads/material usage etc.)
- Anonymous feedback from users shows that the learning materials that have been produced are high quality.

### **Project monitoring**

We propose to monitor and measure this service area against the following indicators:

- The frequency and timeliness of status reports submitted to the DfE on individual projects and the programme as a whole.
- The quality of information given in the status reports, including proposed solutions to addressing any wider barriers to delivery/common issues across multiple projects.

# Strengthening Families, Protecting Children – Project Support Services

Mutual Ventures, Innovation Unit and SCIE are delighted to maintain our successful partnership currently supporting the DfE with the Children's Social Care Innovation Programme and bid to become your support provider for the Strengthening Families Programme.

We believe only our partnership can combine the benefits of continuity with a proven approach to scaling innovation, an established and trusted delivery team, deep technical capability, and a unique ability to hit the ground running to maintain momentum across the programme.

Mutual Ventures and Innovation Unit have provided coaching and technical support to Leeds Family Valued, North Yorkshire's No Wrong Door and Hertfordshire's Family Safeguarding since they first applied to the Innovation Programme in 2014. More recently we have supported the Innovators to prepare their proposals for scaling and spreading their innovations and to develop their initial implementation plans. Accordingly, we have deep understanding of the innovations and have first-hand experience of supporting both Innovators and Adopters to adapt and spread.

SCIE bring national reach within the sector, strength in social work practice, and a strong connection with the What Works Centre to ensure our approach to learning dovetails with the evaluation of the innovations.

Our partnership already has strong, credible and mutually respectful relationships with key stakeholders in each of the innovator sites and a proven ability to work sensitively and successfully with them. We can move quickly to mobilise our support offer with a focused team and proven approach that will respond to the changing needs of the projects over the coming 4+ years.

We are hugely motivated by the opportunity to continue to be part of this effort and maintain the early successes the programme has had in creating step change in practice to transform outcomes for children, young people and families.

As a social enterprise, a charity, and a mutual organisation, committed to public service transformation, our own organisational values and goals align strongly with the success of this programme.

Accordingly, we are delighted to offer a 12% discount on our standard MCF rate card to demonstrate the importance of the programme to us and provide a strong value for money proposition to the department and the sector.

We want to continue to work in genuine partnership with the sector to help continue to use this amazing programme to really transform outcomes for children.

We hope you enjoy reading our proposal.



**David Fairhurst**

Executive Chair

Mutual Ventures



**Matthew Horne**

Deputy Chief Executive

Innovation Unit



**Ewan King**

Chief Operating Officer

SCIE

RESPONSE DOCUMENT

# Strengthening families, protecting children – project support services procurement

Submission from:

**Further Competition from Lot 5 of the Crown  
Commercial Service RM3745 Management  
Consultancy Framework (MCF)**

# ITT Information (for bidder guidance & information)

## INTRODUCTION AND BACKGROUND

The Department for Education reserves the right to request appropriate independent or objective evidence to support supplier responses/statements. Please note that any false statements or information given that is subsequently found to be untrue will automatically disqualify your application and any ensuing contract award.

The criteria set out in the following questionnaire will be used by the ITT Evaluation Panel in conjunction with all other elements of the ITT Procurement Pack to evaluate each application and to compare their relative merits. It is therefore essential that Bidders complete all mandatory sections as fully as possible, and where requested attach supporting documents as evidence of your statements clearly cross referencing to the criteria being evidenced, including page and line numbers where required.

Responses **should not exceed** the word count limit for that particular question or include any embedded / attached documents unless specifically requested. In the event that a response exceeds the word count limit stated for that particular question then all content that follows the maximum word count will be disregarded and will not be evaluated. How Bidders choose to utilise the available word count across the theme is left to their own discretion. Diagrams are acceptable, and will not be included as part of the word count.

**Attachments:** Please ONLY insert attachments where requested to do so. Please only attach documents to the questions as specified. If you insert an attachment to a question that requires a text response, please note your response to the question will **NOT** be marked.

## Instructions

Bidders should complete the questions set out within this document.

## Quality Award Criteria

Bidders are reminded of the Award Criteria which is summarised below detailed within the Document 2 - ITT Process Overview Document.

Question	Weighting
Q1 Experience and Skills	20%
Q2 Project Implementation and Change Management Support	20%
Q3 Supporting Effective Working Relationships	5%
Q4 Spreading of Learning	15%
Q5 Project Monitoring	10%
Q6 Project Plan	5%
Q7 Resources	5%

TOTAL QUALITY	80%
---------------	-----