



Crown
Commercial
Service

Bid Pack for Call-Off Competition

Attachment 5 – Order Contract

Contract Reference: GOV.UK One Login Public Relations Agency

DPS Schedule 6 (Letter of Appointment Template and Order Schedules)

Letter of Appointment

This Letter of Appointment is issued in accordance with the provisions of the DPS Contract (WP2172) between CCS and the Agency, dated Tuesday 20th August 2024.

Capitalised terms and expressions used in this letter have the same meanings as in the Order Incorporated Terms unless the context otherwise requires.

ORDER:

Order Number:	WP2172 GOV.UK One Login PR Agency
From:	Government Digital Service on behalf of Cabinet Office: The White Chapel Building, 10 Whitechapel High Street, London, E1 8QS.
To:	Four Communications Limited, The Hickman Building, 2 Whitechapel Rd, London E1 1FX

Order Start Date:	27th August 2024
Order Expiry Date:	26th August 2026
Order Initial Period:	24 months
Order Optional Extension Period:	12 Months

Goods or Services required:	<p>The Goods and Services under this Order Contract are split into two distinct phases (being Phase I and Phase II) as explained in Schedule 20 (Brief).</p> <p>Goods or Services required for Phase I are set out in DPS Schedule 1 of the DPS Agreement and Order Schedule 20 (Brief) and described as relating to Phase I and are to be delivered in line with the accepted Proposal set out in Schedule 4 and the duly completed Schedule of Works for Phase I attached.</p>
------------------------------------	--

	<p>If Phase II is triggered by the Client giving written notice to the Agency, the Goods or Services to be undertaken are those that are set out in DPS Schedule 1 of the DPS Agreement and Order Schedule 20 (Brief) and described as relating to Phase II and are to be delivered in line with the accepted Proposal set out in Schedule 4 but shall be priced and finalised using the Statement of Works form as per Annex B of this Letter of Appointment.</p>
--	--

Key Staff:	<p>For the Client: REDACTED Under FOIA Section 40, Personal Information</p> <p>For the Agency: REDACTED Under FOIA Section 40, Personal Information</p>
Guarantor(s)	Not Applicable

Order Contract Charges (including any applicable discount(s), but excluding VAT):	<p>The maximum contract value for this contract (including the first phase) will be £670,000 excluding VAT.</p> <p>The maximum contract value for the Phase I will be £70,850 (seventy thousand eight hundred and fifty pounds) excluding VAT. Work will be charged on a time and materials (T&M) basis subject to not exceeding that maximum contract value.</p> <p>Work carried out after Phase I, will be dependent on Cabinet Office approvals and will be on a T&M basis against an agreed rate card (and subject to budget).</p>
Liability	See Clause 11 of the Core Terms (aggregate liability cap under clause 11.2) is £5m (five million pounds)
Additional Insurance Requirements	Not Applicable

Client address billing for invoicing:	<p>Invoices will be sent to:</p> <p>gov.uk-ops@digital.cabinet-office.gov.uk</p> <p>gdsbusinessops@digital.cabinet-office.gov.uk and APinvoices-CAB-U@gov.sscl.com which is at Cabinet Office, PO Box 405, SSCL, Phoenix House, Celtic Springs Business Park, Newport, NP10 8FZ.</p>
--	---

Special Terms	See Special Schedule 9 - Security Management below
----------------------	--

PROGRESS REPORT FREQUENCY

On the first Working Day of each calendar month

PROGRESS MEETING FREQUENCY

Quarterly on the first Working Day of each quarter

KEY SUBCONTRACTOR(S)

Not Applicable

COMMERCIALLY SENSITIVE INFORMATION

Please see the Commercially Sensitive document. Please refer to Joint Schedule 4 (Commercially Sensitive Information).

SOCIAL VALUE COMMITMENT

The Agency agrees, in providing the Goods or Services and performing its obligations under the Order Contract, that it will comply with the social value commitments in Annex A (Order Proposal)

ORDER INCORPORATED TERMS

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

1. This Letter of Appointment includes the Order Special Terms, Order Special Schedules and the Statement of Works for Phase I set out in Annex A.
2. *Joint Schedule 1 (Definitions and Interpretation) RM6124*
3. *Order Special Terms*
4. *The following Schedules in equal order of precedence:*
 - *Joint Schedules for RM6124*
 - *Joint Schedule 2 (Variation Form)*
 - *Joint Schedule 3 (Insurance Requirements)*
 - *Joint Schedule 4 (Commercially Sensitive Information)*
 - *Joint Schedule 7 (Financial Difficulties)*
 - *Joint Schedule 10 (Rectification Plan)*
 - *Joint Schedule 11 (Processing Data)*
 - *Order Schedules for **WP2172 GOV.UK OneLogin PR Agency***
 - *Order Schedule 1 (Transparency Reports)*
 - *Order Schedule 2 (Staff Transfer) - Parts C and E only apply.*
 - *Order Schedule 3 (Continuous Improvement)*
 - *Order Schedule 5 (Pricing Details)*
 - *Order Schedule 6 (ICT Services)*
 - *Order Schedule 7 (Key Agency Staff)*
 - *Order Schedule 10 (Exit Management)*

- *Order Schedule 15 (Order Contract Management)*
- *Order Schedule 20 (Brief)*
- *Annex C to this Letter of Appointment which replaces Order Schedule 9 (and will be referred to as Order Schedule 9 for the purposes of this Order Contract)*

5. CCS Core Terms

6. *Joint Schedule 5 (Corporate Social Responsibility) RM6124*

7. *Order Schedule 4 (Proposal)*. Note however that in terms of priority any parts of the Order Proposal that offer a better commercial position for the Client (as decided by the Client) shall take precedence over the documents in paragraph 4 above for that purpose and to that extent only.

8. Annex B (Statement of Work template)

No other Agency terms are part of the Order Contract. That includes any terms written on the back of, or added to this Order Form, or presented at the time of delivery. For the avoidance of doubt, the relationship between the Parties is non-exclusive. The Client is entitled to appoint any other agency to perform services and produce goods which are the same or similar to the Goods or Services.

FORMATION OF ORDER CONTRACT

BY SIGNING AND RETURNING THIS LETTER OF APPOINTMENT (which may be done by electronic means) the Agency agrees to enter into an Order Contract with the Client to provide the Goods or Services in accordance with the terms of this letter and the Order Incorporated Terms.

The Parties hereby acknowledge and agree that they have read this letter and the Order Incorporated Terms. The Parties hereby acknowledge and agree that this Order Contract shall be formed when the Client acknowledges (which may be done by electronic means) the receipt of the signed copy of this letter from the Agency within two (2) Working Days from such receipt.

For and on behalf of the Agency:		For and on behalf of the Client:	
Signature:	██████████	Signature:	██████████, Under FOIA Section 40, Personal Information
Name:	██████████	Name:	██████████, Under FOIA Section 40, Personal Information
Role:	██████████, Under FOIA Section 40, Personal Information		
Date:	30/08/2024	Date:	02/09/2024

ORDER SCHEDULE 4 (PROPOSAL)

Agency Proposal

This proposal will incorporate the DPS Tender Response

WP2172- GOV.UK One Login- PR Agency- Stage 1b

1.1

GOV.UK One Login is a brilliant new service for our nation and one that needs to be carefully navigated into media and social media conversations to ensure confidence, uptake and security. In moments of major digital and technical change, we, at Four, have been a partner to government departments and public bodies to ensure that at-risk or marginalised audiences are supported and that no one is left behind. Over decades, we have worked on a wide range of technical, digital service launches including the groundwork for the first digitally-led Census, right back to the introduction of Chip and Pin, the cross-sector launch of Paym (with a swathe of reliant parties in the form of high street banks), as well as the Digital Switchover in London (with BBC and Ofcom) which had a specific focus on at-risk and digitally excluded audiences. These campaigns had very similar objectives to the One Login programme - to enable digital transformation, as well as removing barriers to integration.

As a result, we have deep experience in reaching marginalised audiences including those over 70, under 25, or with limited digital access/skills.

In addition, we have a deep experience of fraud and cybercrime, having worked with the Home Office, the NCSC and UK Finance on Cyber Aware and Take Five to Stop Fraud for over ten years. Separately, our team was also involved in the original Lloyds Digital inclusion work and we would bring all of this experience to bear.

STRATEGIC PLANNING AND RESEARCH CAPABILITIES

Our PR planning is supported by insights and award-winning strategists. We use the GCS approved OASIS planning methodology and market leading audience insights tools like Touchpoints, YouGov alongside our own trademarked methodology: Mapper360® to tell us what matters most and what

matters now, to our audiences. Our inhouse skills are supplemented by specialist partners like the BI Team and Furner (who we recently worked with on an Arts Council disability inclusion project) and research agencies like Kantar to understand audiences and build an inclusive approach.

ENSURING APPEAL TO KEY AUDIENCES

Often, with fraud or even tech topics, we are dealing with a low interest topic. People have busy lives and other topics on social media or in the news are more diverting. We need to map the audience's passion points, life stages and geo-location, so that we can link our message to something they do care about, that is relevant to their everyday life. Specialist teams and advisers like BI Team, Furner and our team in Wales - Four Cymru – support in ensuring things are tailored to the audience in

every way. See below for initial insights into the u25 at-risk audience:

See below for initial example insights into the prioritised and at-risk audiences highlighting key channels, influencers and passion points:

[REDACTED] - Under FOIA Section 43, Commercial Interests

A CREATIVE APPROACH TO REACHING DIVERSE AUDIENCES

Our strategy team filters all the information and uses behavioural insights to define the opportunity for the creative team. We explore paid, owned and earned. While this is a PR campaign, boosting of social content can support the reach to diverse audiences. We also co-create with diverse audiences to ensure engagement –

REDACTED- Under FOIA Section 43, Commercial Interests

CAMPAIGN EXECUTION ACROSS VARIOUS CHANNELS

With the right idea, we can reach diverse audiences across a wide range of channels from social media, to local or specialist media, to even private WhatsApp groups – via video content and social cards. Our content needs to be helpful, informative and engaging so that shareability is baked in. Considering the audiences you have highlighted, a mix of social media, traditional media (print, broadcast, online) and in-person events will be key.

[REDACTED] Under FOIA Section 43, Commercial Interests

1.2

CONSISTENTLY ANTICIPATE, MONITOR AND RESPOND TO NEGATIVE PRESS

The Government and public sector campaigns we work on are complex and require careful monitoring and management; we would bring this experience to One Login.

[REDACTED] - Under FOIA Section 43, Commercial Interests

[REDACTED] - Under FOIA Section 43, Commercial Interests

TECHNOLOGY, RESOURCES, AND SUPPORT UTILISED

We use a range of resources including Google alerts, but also media monitoring services like Cision and Onclusive, while **[REDACTED] - Under FOIA Section 43, Commercial Interests**

HOW WE ASSESS AND TRANSFORM PRESS AND SOCIAL MEDIA REACTIONS INTO AN EFFECTIVE MESSAGING STRATEGY

We advise on emerging situations that may or may not turn into media inquiries, [REDACTED] - **Under FOIA Section 41, Information provided in Confidence.** Any questions Four received during media outreach would always be flagged, with responses re-cleared. Our client reports include advice based on listening.

1.3

Our established planning approach will help:

[REDACTED] - **Under FOIA Section 43, Commercial Interests**

Due diligence on influencers is key and we have an established methodology for HMG work.

[REDACTED] - **Under FOIA Section 43, Commercial Interests**

Below is our Mapper methodology for social media influencers:

We've engaged influencers to raise awareness fraud – for the UK Finance Take Five to Stop Fraud campaign. The Trick of the Mind campaign, in 2023, tapped into Gen Z's passion for learning about mysteries of the unknown to show how easy it could be for a criminal to trick them. Activity included, a short online film for socials featuring [Ben Hanlin](#) (TikTok sensation) which was promoted across Meta and TikTok; The Tab media partnership; a suite of content for stakeholders and media outreach. The content reached over 560,000 people, over 4,000 engagements. Across TikTok, 31% of viewers were 18-24 and 26% were 25 – 34, directly reaching our audience.

WP2172- GOV.UK One Login- PR Agency- Stage 2a

2.1

GOV.UK One Login has communications objectives which will help in the overarching aims of preventing fraud among the most vulnerable audiences and increasing digital access for those most marginalised.

The communications campaign will deliver on the aims if we drive engagement by elevating understanding from 'another digital service' to a narrative around One Login as 'THE' powerful tool to create make life easier for yourself, your family, local community and a service that will save money for the nation but one that, as a result, needs special care. The ultimate mark of success will be to personalise One Login, focusing on emotional triggers to drive engagement, while using rational facts to make it indisputably useful and valued – and protected from fraud.

There is an opportunity to create a highly positive and shared experience for One Login that includes marginalised people from every region, culture, faith and age across the nation.

The main challenges will be:

- Salience – people have short attention spans and have busy, sometimes difficult lives. Making One Login relevant is key
- Getting the balance of broader segmentation and micro-targeting right. Reach is important but it will be vital to understand and address the blocks and levers to our One Login marginalised audiences
- The looming General Election means an ability to flex to handle this will be vital

Our insight-led, integrated planning starts with a persona-first methodology to understand context and identify strategy and tactics. We will build data rich personas for your key marginalised audiences. Examples below:

██████████ - Under FOIA Section 41, Information provided in Confidence

As you can see our profiles give us a strong jumping off point for mapping the most influential media, a steer on geographies, but also on passion points and charities or stakeholders that will engage our key audiences.

Our approach is underpinned by behaviour change frameworks (COM B) allowing us to understand issues, identify barriers - both internal (e.g. bias) or external (e.g. societal norms) - and calculate how best to overcome them.

Our established planning approach will help:

1. Understand the landscape around One Login
2. Map the services most applicable to age ranges and marginalised audiences – to drive salience
3. Map the influencers and stakeholders around each of these – to generate influence
4. Identify what nudges can be delivered through, identifying ‘moments that matter’ around mental or physical availability
5. Establish the proposition to unify the consumer truth.

We evolve this into campaign planning following the OASIS model. An organising idea will inform the creative approach and seek to answer:

1. What are the messages and vehicles to deliver both niche targeted and mass awareness?
2. Which touchpoints are most effective?
3. Who are the influencers that resonate most with the audience?
4. What are the passion points for the audience, informing the capability for both hyper targeted and large scale partnerships?

When targeting hard-to-reach audiences we will also explore:

██████████ - Under FOIA Section 41, Information provided in Confidence

We will analyse your insights on the specific risks of fraud, any particular points of incidence and behaviours to promote amongst the most vulnerable audiences. We will then build this into our planning. **██████████ - Under FOIA Section 41, Information provided in Confidence**

For UK Finance, **██████████ - Under FOIA Section 41, Information provided in Confidence**

Our MoJ campaign (PR Week Award winner 2023), **██████████ - Under FOIA Section 41, Information provided in Confidence**

2.2

We centre our audiences in several ways from strategy, insights and creative development through to execution.

Our team includes analysts and strategists who turn information into insight that power effective, accountable strategies to drive change, linked to policy outcomes among a defined audience. We align creative, message and mode of delivery to the audience. We develop and validate a segmentation approach appropriate to the objective, strategic challenge and communications task.

██████████ - Under FOIA Section 41, Information provided in Confidence.

Our own methodology: Mapper360® provides a layer of actionable psychographic, behavioural and demographic data. It uses open-source data as its huge, real-time dataset and with a combination of licensed software and expert analysts, can analyse online behaviour, content and conversational activity. This delivers insights at scale for mass audiences and for niche/specialist audiences, supplementing traditional research techniques such as depth interviews and focus groups (vital for understanding some harder to reach groups).

[REDACTED] - Under FOIA Section 41, Information provided in Confidence

Our audience insights are shared with our creative and PR teams and ideas are developed based on a clear creative brief. Audience insights provide such fertile ground for concepts, even to the point of featuring 'real people' or case studies and quotes to bring the message to life. We often co-create with a working group that represent our audiences or test our ideas with focus groups based on the audience segments or with stakeholders that represent the audiences like Age UK. This provides a useful filter and feedback loop, and we would also 'listen' while the campaign is live monitoring comments, and positivity vs negativity from the audiences for One Login.

2.3

We have years of experience monitoring and managing coverage for clients in emerging situations and for sensitive policy areas

[REDACTED] - Under FOIA Section 41, Information provided in Confidence

TRIAGING

First we agree a set of topics to monitor for and then we build the reporting rhythms and methodology. Once this is in place, we know what to report on, when and we will always provide insight and advice. Because of our experienced team, we add can value beyond the obvious and flag emerging topics.

MANAGING NEGATIVE PRESS

Our experience of working with press office teams within Government

[REDACTED] - Under FOIA Section 41, Information provided in Confidence

2.4

BALANCING CREATIVITY AND INNOVATION WITHIN CONSTRAINTS

We understand the challenges faced by Government press office teams **[REDACTED] - Under FOIA Section 41, Information provided in Confidence**

It's not easy, but we can still deliver creative, impactful campaigns that make a difference for our audiences. For us at Four, creativity and innovation is often borne out of constraints and we prefer to focus on solutions and workarounds, rather than problems. As an agency that works with a wide range of Government departments on policy areas from education to fraud, and PR Weeks Number 1 public sector agency, we bring new ideas that adhere to the parameters of Government communications. Our insights and strategy planning model gives us rich territory for the

development of creative ideas. We still undertake a traditional creative and innovative process and focus but we then apply filters to ensure that ideas are 'fit for purpose' within the context of campaigns that are publicly funded. This includes due diligence on any stakeholders or influencers that we ask to back the campaign.

MANAGING THE CONVERSATION USING THIRD PARTIES

We regularly engage with third parties for our government campaigns and are experienced in having to design our engagement process so that we do enough to excite them about the campaign while also managing expectations and the real possibility that launches can get postponed.

2.5

As an agency with deep experience in public sector PR campaigns we understand the importance of accountability with budgets, deliverables and timings being carefully tracked and transparently reported to our client teams.

We tailor our reporting methods to each clients' requirements.

[REDACTED] - Under FOIA Section 41, Information provided in Confidence

We can also do this for any inter-agency work or to map the lines of work between GDS One Log In, Cabinet Office and our own team. We are very familiar with working on RACI matrices and this is core to our way of working and managing quality control with clients, including our international work with Defra. This format enables us to itemise every part of a campaign plan to include all sub-contractors, partner agencies and wider customer team. Visually we include this on a campaign GANTT chart for clear visual working whilst still highlighting detailed tasks.

Client satisfaction is formally reviewed and measured by the project manager on a regular basis to ensure that any challenges are effectively dealt with, and that client satisfaction is maintained. The contract manager and senior members of the core team are available to escalate and manage any issues that arise. This begins with risk mitigation at the start of any contract or campaign and the categorisation of any risks to the project based on likelihood and severity of impact, followed by mitigating actions. For these, and unforeseen issues, the team are available 24/7 to react, and have experience of working with departmental communications teams, ministerial advisers and Cabinet Office.

WEEKLY: The account director provides a weekly at-a-glance action-oriented status report and updated project timeline. It can include the percentage of resources used and percentage of milestones complete between the agency and GDS, with an activity dashboard.

MONTHLY: Strategy meetings for which an agenda and status report will be produced and sent to you 48 hours in advance. These meetings are run by the account director with attendance of team members. A contact report detailing actions arising from this session will be sent to you within 48 hours.

QUARTERLY REVIEWS: These will be used as a moment to fully review the delivery of the campaigns against the KPIs, to discuss weak points and opportunities and to examine ways of working including service levels.

Example dashboards:

[REDACTED] - Under FOIA Section 41, Information provided in Confidence

2.6

HEALTHY WORKING CULTURE

We are an open and engaged team. We want to do great work and part of this is about having strong client relationships - we supplement formal meeting structures with informal catch ups with campaign managers to ensure we are always on the front foot. We prioritise health and wellbeing, with mental health first aiders on staff and we have a pragmatic approach to tackling challenges as one team – client and agency together.

MAINTAINING A CULTURE OF IMPROVEMENT AND ITERATION

No two days are the same in PR and certainly not in Government communications. We are ready for anything. We do this by:

Monitoring the media, engaging with our community influencers to hear what they have to say, analysing social media – all of this helps us to either identify issues before they escalate or - when issues occur - understand reactions to map a way through.

Putting senior, strategic minds to work – our team includes some of the most experienced Government communicators in the UK – together there is not much we haven't tackled and we have learnings and insights to bring. But we don't have egos – we just want to deliver good work and contribute to the One Login mission.

Sharing learnings from previous challenges – being honest about failures as well as what worked.

ENSURING DIVERSITY AND INCLUSIVITY

Our team is made up of people from a wide variety of backgrounds – this helps with resolving challenges, but we also understand the political, legal and social elements of diversity. We've worked on a range of EDI campaigns for Innovate UK, Lloyds and others. This allows us to build a communications strategy on strong foundations. Part of our Employee value proposition includes staff groups on Race Equality, Gender Equality and Pride – these groups also input into our campaigns.

2.7

We prefer to act as an extension of the GDS One Login team as we have done for Home Office, MoJ, FCOD, DfE over the years. Our team will understand the pressures facing your team and will meet you play for play, each day. Reading the requirement, we can see that the GDS One Login team has both its own press team and a close reporting line to Cabinet Office press office. We have operated in similar structures before. Collectively, our team has decades of experience of working with government and public sector – we are structured in managing relationships and reporting; while flexible and pragmatic.

[REDACTED] - Under FOIA Section 41, Information provided in Confidence

With Four, you would be supported by a team that understands the mission that One Login is building towards and can support in navigating the way through. We are deeply experienced in Cabinet Office approved methodologies. Our position on the RM6125 roster gives us regular access to GCS and Cabinet Office and insights from senior personnel.

We understand that while there are guard rails in place we must also be alive to the wider context and that guidance can move with the poles of the landscape.

WP2172- GOV.UK One Login- PR Agency- Stage 2a: SOCIAL VALUE

2.8

We are working towards zero carbon emissions and undertake an annual review of operations and their effect on the environment, this includes reporting Scope 1, Scope 2 and Scope 3 data, using the SECR¹.

Almost all our energy used comes from renewal sources; we do not have a car fleet and encourage public transport usage and walking where possible; we use recycled and environmentally preferred office supplies. We will deliver environmental benefits by conducting pre-contract engagement activities with a diverse range of organisations to support us including Ecovadis, and Climate Impact Partners to report on: The percentage of carbon reduction (measured in MTCDE across Scope 1, Scope 2 and Scope 3 that we are committed to and the date by which we are committed to carbon Net Zero at a corporate level. This will independently verified informed by our work with Climate Impact Partners, as will our reporting on the percentage of decarbonisation roadmap reliant upon carbon offsetting to achieve Net Zero commitments. It will also allow us to establish, implement and track an environmental scorecard which measures a range of strands.

In the next six months we are introducing a new Agency sourcing and reporting policy which will monitor environmental and ethical information about our key supply chain partners including media channels. We have a staff-led group, Four Earth, which works with the operations team on environmental initiatives, volunteering and supporting clients with initiatives like implementing dark mode design work, carbon neutral media buying and more.

1

<https://www.gov.uk/government/publications/academy-trust-financial-management-good-practice-guides/streamlined-energy-and-carbon-reporting>

2.9

Four has a long-term EDI strategy which is designed to tackle inequality in employment, skills and pay; including commitments for recruitment, training and creative output. We work with The Taylor Bennett Foundation, Black Professionals Network and Spark! to attract more diverse candidates. We roll out annual diversity training via Equaliteach and this ensures our teams are upskilled in delivering work and influencing staff, users and partners to support people with disabilities of all kinds. We fund and support staff-led groups on Gender Equality, Pride and Race Equality. These groups organise events throughout the year and have direct access to the Board. They also advise on topics, help design campaigns, and hold us to account.

This approach cascades into our delivery of work and we are engaged at GCS-level and with leaders in the field like our client Channel 4 on inclusive design and we would extend this to working with GDS designers to make designs accessible, inclusive and equitable for all users.

We are a registered Disability Confident Level 1 Committed employer and within the development of our Disability Pledge, we're guided by the UN Disability Strategy. Our office has the highest accessibility standards. We support employees who are neurodiverse or with different types of disability, through working with our IT and Operations teams to provide tech solutions. We work with client teams to ensure meetings are inclusive for those living with different abilities including in the choice of venue, the sound and vision and in considering those who are immunocompromised.

COMMERCIAL ENVELOPE COMMENTARY

INTRODUCTION

We have put forward a team with the skills, experience and seniority to deliver for GDS One Login. These team members all have experience on working with Government departments to deliver complex messaging to at risk and minoritised audiences during high profile, high pressure moments including reporting into Cabinet Office. The team has worked on major public sector digital launches and media moments for Government and has an innate understanding of the mood of the nation, the temperament of media and the messages that influence.

RATES

Our rates represent excellent value for money but also a high level of seniority and experience.

ROLES FOR THE REQUIREMENTS OF PHASE 1

We have included a team that will deliver intelligent insights, strategy, planning and PR excellence. An award-winning team, that is rated as the number one public sector agency by PR Week – this is the best of the best.

[REDACTED], Under FOIA Section 40, Personal Information, chief strategy office,
[REDACTED], Under FOIA Section 40, Personal Information, director and
[REDACTED], Under FOIA Section 40, Personal Information,
[REDACTED], Under FOIA Section 40, Personal Information

We have allocated a healthy amount of time to strategy and insights – with

[REDACTED], Under FOIA Section 40, Personal Information, supported by analyst
[REDACTED], Under FOIA Section 40, Personal Information. This can be upweighted if required, depending on the rhythm of social media analysis and reporting required.

Beyond the roles, highlighted in the rate card, we have upweighted at both a senior and junior level to ensure that we offer both the experience in the broadest sense of the overall ambitions of One Login and also the detailed knowledge of media monitoring from our executives who provide that administrative support day in day out to Government clients from MoJ and DfE to Home Office. This will help us to quickly mobilise and get under the skin of the brief.

Specifically [REDACTED], Under FOIA Section 40, Personal Information
[REDACTED], Under FOIA Section 40, Personal Information

WP2172 GOV.UK One Login PR Agency- Commercial: Value

2.10

Proposed Team Schedule

Unique individual	Job role / title (please enter)	level of experience 1-4 (where 1 = junior, 2 = Middle Lower, 3 = Middle Higher, 4 = Senior. 5= Department Head	day rate excl. VAT (inclusive of x,y,z)	Agency to specify the estimated no. of days they will spend on first-stage of the project, including iterations following research, client meetings & presentations etc (up to (x) days)	total cost of team member on project
Under FOIA Section 40, Personal Information	Director	Under FOIA Section 43, Commercial Interests	Under FOIA Section 43, Commercial Interests	Under FOIA Section 43, Commercial Interests	Under FOIA Section 43, Commercial Interests
Under FOIA	Creative	Under FOIA Section 43,		Under FOIA	

Section 40, Personal Information		Commercial Interests	- Under FOIA Section 43, Commercial Interests	Section 43, Commercial Interests	- Under FOIA Section 43, Commercial Interests
Under FOIA Section 40, Personal Information	Analytics, Planning & Strategy	- Under FOIA Section 43, Commercial Interests	- Under FOIA Section 43, Commercial Interests	- Under FOIA Section 43, Commercial Interests	- Under FOIA Section 43, Commercial Interests
Under	Analytics, Planning &	- Under FOIA Section 43,	- Under FOIA	- Under FOIA	- Under FOIA

FOIA Section 40, Personal Information	Strategy	Commercial Interests	- Under FOIA Section 43, Com merc ial Inter ests	Section 43, Commercial Interests	- Un de r FO IA Sec tio n 43, Co m me rc ia l Int ere sts
Under FOIA Section 40, Personal Information	Senior Project Manager	- Under FOIA Section 43, Comm ercia l Inter ests	- Under FOIA Secti on 43, Com merc ial Inter ests	- Under FOIA Section 43, Commercial Interests	- Un de r FO IA Sec tio n 43, Co m me rc ia l Int ere sts
Under	Account	- Under FOIA Section 43,	-	- Under FOIA	£4,800.00


FOIA Section 40, Personal Information	Executive	Commercial Interests	- Under FOIA Section 43, Commercial Interests	Section 43, Commercial Interests	
REDACTED-		- Under FOIA Section 43, Commercial Interests	- Under FOIA Section 43, Commercial Interests	- Under FOIA Section 43, Commercial Interests	- Under FOIA Section 43, Commercial Interests
REDACTED-		- Under FOIA Section 43, Commercial Interests	- Under FOIA Section 43,	- Under FOIA Section 43, Commercial Interests	- Under FOIA

			Com merc ial Inter ests		Sec tio n 43, Co m me rci al Int ere sts
					£0.00
Total cost of proposed team			RED ACTE D- Unde r FOIA Secti on 43, Com merc ial Inter ests	REDACTED- Under FOIA Section 43, Commercial Interests	RE DA CT ED - Un de r FO IA Sec tio n 43, Co m me rci al Int ere sts
Vs first-stage budget					88.56%


2.11

Rate card for specified roles

Role #	Department	Role Descriptor	Role Breakdown	Suggested years of experience	Rate (£)
1	Account Management	Middle (Upper)	Second in command on the management of an account. Deputy in the client-facing role and highly operational. Reports into account lead such as account director.	5 years+	<div style="background-color: yellow; padding: 5px;"> <div style="background-color: black; width: 100px; height: 100px; margin-bottom: 5px;"></div> <div style="text-align: center;"> - U n d e r F O I A S e c t i o n 4 3 , C o m m e r c i a l </div> </div>

					a l l i n t e r e s t s
					
			Typically works to a brief set to them by a creative director with a remit to originate ideas for the brief for approval by the creative director.		- U n d e r F O I A S e c t i o n 4 3 , C o m m e r
4	Creative	Middle (Upper)		5 years+	

					cial Interests
5	Creative	Junior	<p>More of an internal-facing role, sometimes working to a brief set to them by a creative director with a remit to originate ideas for approval by the creative director. Often providing day to day support to more senior creative teams.</p>	Up to 3 years	<div></div> <p>- Under FOIA Section 43, Commerce</p>

					e r c i a l I n t e r e s t s
			Undertakes research, provides insight on strategy and approach. Creates integrated communications strategies and carries out evaluation and analysis.		 - U n d e r F O I A S e c t i o n 4 3 , C o m
7	Analytics, Planning & Strategy	Middle (Upper)		5 years+	

					m e r c i a l I n t e r e s t s
--	--	--	--	--	--

2.12

CVs

ACCOUNT MANAGEMENT

██████████ - Under FOIA Section 40, Personal Information

ANALYTICS, STRATEGY AND PLANNING

██████████ - Under FOIA Section 40, Personal Information

CREATIVE

██████████ - Under FOIA Section 40, Personal Information

Annex A

Statement of Works for Phase 1

This Statement of Work is issued under and in accordance with the Order Contract entered into between the parties dated *[insert date of signature of Order Contract.]*

WP2172 GOV.UK One Login PR Agency One Login -Phase I Statement of Work

Attachment 5- Annex A Statement of Work (SOW), including pricing arrangements and Key Staff

SOW Details

Date of SOW: <i>TBC</i>
SOW Reference: <i>WP2172</i>
Client: <i>The Cabinet Office- GDS</i>
Supplier: <i>Four Communications Ltd</i>
Release Type(s): <i>Marketing and Communication</i>
Phase(s) of Delivery: <i>Phase I</i>
Release Completion Date: <i>TBC</i>
Duration of SOW <i>TBC</i>
<i>Time and Materials subject to the Capped</i> Charging Method(s) for this

Value
Release:

- 1.1 The Parties will execute a SOW for each Release. Note that any ad-hoc Service requirements are to be treated as individual Releases in their own right (in addition to the Releases at the delivery stage); and the Parties should execute a separate SOW in respect of each.
- 1.2 The rights, obligations and details agreed by the Parties and set out in this SOW apply only in relation to the Services that are to be delivered under this SOW and will not apply to any other SOW's executed or to be executed under this Call-Off Contract unless otherwise agreed by the Parties.

Key Staff

- 1.3 The Parties agree that the Key Staff in respect of this Project are detailed in the table below.- To be concluded

1.4 Table of Key Staff:


Name	Role	Details
██████████ Under FOIA Section 40, Personal Information	Head of Communications (GOV.UK One Login)	Project owner - key person responsible for deliverables on SOW. Sets direction and standards on products produced by the agency ensuring join up with branding projects and wider GDS comms.
██████████ Under FOIA Section 40, Personal Information	Deputy Director - Digital Identity	Senior sign off on media strategy, budget allocation. Ensures strategic alignment of One Login comms alongside wider programme considerations.
██████████ Under FOIA Section 40, Personal Information	Director, Digital Identity	Senior Responsible Owner for One Login delivery Primary sign off and stakeholder in media approach

Under FOIA Section 40, Personal Information	Communications Manager	Project support - coordination on timelines, agency support and content creation + press office coordination
Under FOIA Section 40, Personal Information	Senior Strategy and Policy Advisor	Primary contact for stakeholder connection + engagement
Under FOIA Section 40, Personal Information	Head of Customer Strategy	Primary contact for Reliant Parties (RPs) - defined as government departments whose services are using One Login
CO press office	CO press office	Provide access to media cutting service Receive insight / flags in coverage + analysis briefing Sighted on stakeholder engagement (via One Login comms) Press office to handle gridding process and timelines NB - relationship with agency will be primarily via One Login comms. Initial kick off introductions between press office / agency will be arranged


Deliverables

1.4 Phase I of the Services, as identified in Order Schedule 20, ("Phase 1") that the Agency will deliver under this Order Contract will include each of the Milestone Deliverables as described and identified in the table below. Each Milestone Deliverable will incorporate the activities, tasks, outcomes and other matters set out under the column "How measured/accepted" which occupy the same numbered row of the table as that Milestone Deliverable. The column headed "Due Date" indicates estimated duration, timings and conditions for each of the Milestone Deliverables and also sets out apportionment of the Agency's Capped Value against each of the Milestone Deliverables.



We have provided a [Gantt chart](#) to give an indicative view of how all the following tasks would be programmed in Phase I, but the Client may amend and modify from time to time the timings of the respective tasks shown in the chart to meet programme needs. The Client will seek to collaborate with the Agency to agree the timings.



Deliverable Number	Milestone Deliverable	How measured/accepted	Due Date
#1	Establish partnership working within One Login team	<ul style="list-style-type: none"> - Induction week attendance and engagement - Present to internal groups on Four background, role and scope - Collaborate on strategic priorities with One Login team, agreeing a firm outline of work within time and budget - Agree ways of working - ideally 2x weekly check in + monthly review - Establish effective working relationship with press office through initial meeting + agreed ways of working and regular contact (via One Login team) <p>Output:</p> <ul style="list-style-type: none"> - Project plan and objectives 	<p>Week 1-2 of project</p> <p>(Supplier to bear costs)</p>
#2	Develop and agree strategy and additional insights	<p>The below lists work / activity which would be expected to be conducted to contribute to the drafting of the below outputs. The supplier can add / remove activity as appropriate in order to deliver the outputs. Standards will be agreed through regular checkpoints.</p> <ul style="list-style-type: none"> - Review all provided One Login insights and evidence (UCD audience insight, Data and Analytics, Benefits information, Brand testing and insight, GOV.UK polling, existing media monitoring) 	<p></p> <p>- Under FOIA Section 43, Commercial</p>

		<ul style="list-style-type: none"> - Review and build on all provided One Login material and plans including crisis plan, stakeholder engagement plan, comms plan - Agency to conduct interviews as appropriate (suggested participants include: (1) Head of Customer Engagement to understand RP relationship / opportunities; (2) Head of UCD to understand audiences; (3) Senior engagement manager to understand current relationships / external perception/ risks; (4) additional volunteer partners / potential partners to identify opportunities) - Agency to conduct further desk research with open source material + owned Four resources - Agency to provide analysis and recommendations on gaps + opportunities for additional insight, using existing evidence where possible and using contracts to conduct further insight - Attend One Login external advisory group as observers, where comms campaign/brand will be discussed <p>Output:</p> <ul style="list-style-type: none"> - Audience profiles - Media Strategy inc. channel recommendations and potential influencers with recommendations on appropriateness and reach - Press office to see and approve media strategy - PR plan including proactive, reactive and crisis management - Press office will continue to handle all reactive comms 	Interests
--	--	--	------------------

		<ul style="list-style-type: none"> - Additional YouGov and Touch point insights as needed 	
#3	Set up media monitoring including early monitoring plan/ crisis management, implementation + reports	<ul style="list-style-type: none"> - Work with team to agree key words / focus / approach and objectives for media monitoring - Provide detailed daily media, social media, reports - Monthly strategic reviews of coverage and conversation with appropriate recommendations on adjustments in overall strategy - Continuous tracking of social media, news, and forums for ongoing sentiment and potential crises, with real-time alerts - Real-Time Alerts: Immediate notifications for identified crisis indicators to the One Login team - Risk Assessment: Analysis to identify potential crises and their impact on the public as well as suggested overall strategy and tactics for response - Media & Messaging: Working with the One Login team and the Cabinet Office the agency will need to create messages to use across channels. A standard set of messaging can be created in advance and used as needed and will be managed by the One Login team. Other issues around this may require additional messaging work. - Digital Media Engagement advice: Best practice of the crisis narrative on digital channels such as social platforms, forums, blogs etc - Continuous Improvement and reporting: Ongoing monitoring and refining of crisis strategies and reporting regularly (fortnightly as a minimum or more often as required) on changes in activity 	 <p>- Under FOIA Section 43, Commercial Interests</p>

		<p>Output:</p> <ul style="list-style-type: none"> - Continuous monitoring and real time alerts - Real time advice depending on issue - Daily media, social media reports for 3 months - 3 final monthly reports with analysis, and recommendations - to build cumulatively on monthly reports for overarching narrative - Review and refinement of crisis plan 	
#4	Stakeholder mapping	<ul style="list-style-type: none"> - Desk research of provided documents + Four sourced information on relevant stakeholders and context - 1-1 interviews as appropriate for depth of stakeholder consideration - Host workshop with 3 distinct set of stakeholders to define the Stakeholder Engagement strategy and identify outputs <ul style="list-style-type: none"> - RPs - Voluntary sector - Public sector <p>Outputs</p> <ul style="list-style-type: none"> - Hosted 3x workshops - Stakeholder strategy map - Engagement plan - Content plan 	<p>Approx 3-4 weeks - to commence after audience profiles and insight gathering tasks comprised within row 2 have been completed (as confirmed by GDS).</p>

			 - Under FOIA Section 43, Commercial Interests
#5	Message development	<ul style="list-style-type: none"> - analysis of existing messages, key data points - host message development session (Comms, Engagement, Policy, UCD) - Creation of messaging house - Follow up session to finalise messages <p>Output</p> <ul style="list-style-type: none"> - 3 key messages and reasons to believe to guide PR and stakeholder work 	 - Under FOIA Section 43, Commercial Interests

#6	Stakeholder engagement	<ul style="list-style-type: none"> - Production of stakeholder tool kit for 3x distinct groups of stakeholders with ability to be tailored to individual audiences <ul style="list-style-type: none"> - Volunteer - RP - Public sector - Ongoing stakeholder engagement with direct connection and coordinated promotion of One Login - Press office to be cited on language and activity with opportunity to raise major flags <p>Outputs</p> <ul style="list-style-type: none"> - 4-5 months of stakeholder engagement - 3x tool kits (to include information on One Login + social media, calendar, gifs, newsletter, web copy and case studies as appropriate) - 10-15 stakeholder outputs endorsing One login / sharing content - Evaluation of effectiveness of activity 	<p>Timing of proactive promotion within the outputs will be dependent on GDS notifying the Agency (which is contingent on programme needs)</p> <p></p> <p>- Under FOIA Section 43, Commercial Interests</p>
#7	Press engagement	<ul style="list-style-type: none"> - Engage, react, and proactively interact with the chosen targeted audience on behalf of the GDS One Login team via agreed routes - Recommend opportunities for media placement or interviews with Ministers or other government officials and programme leads. - Leveraging targeted, high-impact media outlets/groups outside of mainstream media. - 4-5 months of drumbeat proactive and reactive PR including lines to take, 	<p>Timing will be subject to GDS notifying the Agency, based on development of programme demands - likely to commence from July</p> <p></p>

		<p>development of media lists, press, materials, Press office engagement</p> <ul style="list-style-type: none"> - press office to approve all proactive activity in advance <p>Output</p> <ul style="list-style-type: none"> - 20 - 25 pieces of coverage of positive / neutral sentiment - prepared lines to take 	Under FOIA Section 43, Commercial Interests
#8	Reporting	<ul style="list-style-type: none"> - Analysis of campaigns, outlining effectiveness- via agreed key metrics. outlining insights for future improvements. 	Throughout the anticipated first phase of the contract.

Milestone Deliverables will be mandatory within each Statement of Work and will be reviewed regularly throughout the contract and may potentially be amended at the end of each month.

Sch 3.4 Call-Off Contract Charges

3.4.1 The charges for Phase I will be calculated on the basis of the rates set out in Order Schedule 5 (Pricing Details) (and evidenced accordingly) but subject to a maximum capped amount of £70,850 (seventy thousand eight hundred and fifty pounds) (excluding VAT and expenses) which sum shall be referred to as the “Capped Value”.

3.4.2 The Agency shall not be entitled to recover from the Client any charges in excess of the Capped Value.

3.4.3 The Agency shall also not be entitled to be paid any expenses it incurs in relation to the Services under this SOW, except to the extent that such expenses have been agreed in writing at the date of this SOW including the limit of the amounts that are recoverable from the Client in respect of each expense type. The Agency shall be solely responsible for bearing the costs of any expenses in excess of such limits and shall not seek reimbursement from the Client in respect of such excess.

3.4.4 The Client is not able to commit to proceed to Phase II of the Services as described in Order Schedule 20 ("Phase II") under this Order Contract and gives no assurance or warranty in respect of Phase II, whether in whole or in part or whether engaging the Agency or otherwise. The Client reserves its entitlement to choose to undertake the relevant activities intended to be comprised in Phase II itself or to engage some other third party to do so. The Agency acknowledges that no such assurances have been given and agrees that it has no entitlement in respect of Phase II unless and until (and then only to the extent specifically provided) a further Statement of Work is entered into between the Client and the Agency in respect of Phase II.

Sch 3.5. Agreement of statement of works

BY SIGNING this SOW, the Parties agree to be bound by the terms and conditions set out herein:

For and on behalf of the Supplier:

Name and title

 _____

Signature and date

For and on behalf of the departmental Client:

Name and title

Signature and date

Annex B

Statement of Work

This Statement of Work is issued under and in accordance with the Order Contract entered into between the parties dated *[insert date of signature of Order Contract.]*

Any schedule attached to this Statement of Work will describe in detail the different types of Services to be provided under that Statement of Work. A schedule attached to this Statement of Work only applies to the relevant project to be delivered under that Statement of Work, and not to any other Statement of Work, or to the provision of the Services as a whole.

1.1 Where a Statement of Work would result in:

- a variation of the Services procured under this Order Contract; •
- an increase in the Charges agreed under this Order Contract; or
- a change in the economic balance between the Parties to the detriment of the Client that is not provided for in this Order Contract, the relevant term(s) will be dealt with as a proposed Variation to this Order Contract in accordance with the Variation procedure set out in Clause 24.

[Note: Template content from RM6124 below to be developed for each Statement of Work as required]

WP2172 GOV.UK One Login- PR Agency

The purpose of this project is to provide active engagement around the benefits of GOV.UK One Login programme

[To be completed]

N/A

N/A

[To be completed]

Services captured within Order Schedule 20- Brief

To be agreed during Project kick-off sessions

Total cost of proposed team

£

Charges will be calculated using the hourly charge out rates shown in Order Schedule 5 for Phase II.

Set out details of the materials or information to be provided to the Agency.

If Services are to be supplied outside the UK, specify additional territories here

Not applicable

Set out any special terms that are intended to take precedence over the Order Terms and/or the Schedules to the Order Terms such as, security requirements, warranties, specific insurance requirements, any specific data reporting requirements etc.

Chief Executive- [REDACTED] Under FOIA Section 40, Personal Information

Director- [REDACTED] Under FOIA Section 40, Personal Information

Creative- [REDACTED] Under FOIA Section 40, Personal Information

Analytics, Planning & Strategy- [REDACTED] Under FOIA Section 40, Personal Information

Analytics, Planning & Strategy- [REDACTED] Under FOIA Section 40, Personal Information

Senior Project Manager- [REDACTED] Under FOIA Section 40, Personal Information

Account Executive- [REDACTED] Under FOIA Section 40, Personal Information

Please see "Key Staff" above.

Please see "Key Staff" above.

Order Schedule 9- Security Management

1 Client Options

Risk assessment

The Client has assessed this Agreement as	a standard consultancy agreement	<input checked="" type="checkbox"/>
	a higher-risk consultancy agreement	<input type="checkbox"/>

Relevant Certifications

Where the Client has assessed this Agreement as a standard consultancy agreement, it requires the Agency to be certified as compliant with:	Cyber Essentials	<input checked="" type="checkbox"/>
	Cyber Essentials Plus	<input type="checkbox"/>

2 Agency obligations

- 2.1 Where the Client has assessed this Agreement as a higher-risk consultancy agreement, the Agency must comply with all requirements in this Schedule 1 (Security Management).
- 2.2 Where the Client has assessed this Agreement as a standard consultancy agreement, the Agency must comply with this Schedule 1 (Security Management), other than:
- (a) the requirement to be certified as compliant with ISO/IEC 27001:2013 under Paragraph 7.1(b);
 - (b) the requirement to undertake security testing of the Agency Information Management System in accordance with paragraph 3 of Appendix 1;
 - (c) the requirement to produce a Security Management Plan in accordance with Paragraph 8
 - (d) the requirement to document unencrypted Client Data in the Security Management Plan in accordance with paragraph 5.4 of Appendix 1

3 Definitions

In this Schedule 9 (Security Management):

“Anti-virus Software”	means software that: protects the Agency Information Management System from the possible introduction of Malicious Software;
------------------------------	---

	<p>scans for and identifies possible Malicious Software in the Agency Information Management System;</p> <p>if Malicious Software is detected in the Agency Information Management System, so far as possible:</p> <p style="padding-left: 40px;">prevents the harmful effects of the Malicious Software; and</p> <p style="padding-left: 40px;">removes the Malicious Software from the Agency Information Management System.</p>
<p>“Breach of Security”</p>	<p>means the occurrence of:</p> <p style="padding-left: 40px;">any unauthorised access to or use of the Services, the Client Premises, the Sites, the Agency Information Management System and/or any information or data used by the Client, the Agency or any Sub-contractor in connection with this Agreement;</p> <p style="padding-left: 40px;">the loss (physical or otherwise) and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Client, the Agency or any Sub-contractor in connection with this Agreement; and/or</p> <p style="padding-left: 40px;">any part of the Agency Information Management System ceasing to be compliant with the Certification Requirements.</p>
<p>“Client Data”</p>	<p>means any:</p> <p style="padding-left: 40px;">data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media; or</p> <p style="padding-left: 40px;">Personal Data for which the Client is a, or the, Data Controller,</p> <p>that is:</p>

	<p>supplied to the Agency by or on behalf of the Client; or</p> <p>that the Agency generates, processes, stores or transmits under this Agreement.</p>
“Client Equipment”	means any hardware, computer or telecoms devices, and equipment that forms part of the Client System.
“Client System”	means the information and communications technology system used by the Client to interface with the Agency Information Management System or through which the Client receives the Services.
“Certification Default”	means the occurrence of one or more of the circumstances listed in paragraph 7.4.
“Certification Rectification Plan”	means the plan referred to in paragraph 7.5(a).
“Certification Requirements”	means the information security requirements set out in paragraph 7.
“Cyber Essentials”	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme.
“Cyber Essentials Plus”	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme.
“Cyber Essentials Scheme”	means the Cyber Essentials scheme operated by the National Cyber Security Centre.
“End-user Device”	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services.
“HMG Baseline Personnel Security Standard”	means the employment controls applied to any individual member of the Agency Personnel that performs any activity relating to the provision or management of the Services, as set out in “HMG Baseline Personnel Standard”, Version 6.0, May 2018

	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf), as that document is updated from time to time.
“Malicious Software”	means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations.
“NCSC Cloud Security Principles”	means the National Cyber Security Centre’s document “Implementing the Cloud Security Principles” as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles .
“NCSC Device Guidance”	means the National Cyber Security Centre’s document “Device Security Guidance”, as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance .
“Privileged User”	means a user with system administration access to the Agency Information Management System, or substantially similar access privileges.
“Process”	means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data.
“Prohibited Activity”	means the storage, access or Processing of Client Data prohibited by a Prohibition Notice.
“Prohibition Notice”	means a notice issued under paragraph 1.3 of Appendix 1.

“Relevant Certifications”	means those certifications specified in paragraph 7.1.
“Relevant Convictions”	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), or any other offences relevant to Services as the Client may specify.
“Security Management Plan”	means the document prepared in accordance with the requirements of paragraph 8.
“Sites”	<p>means any premises:</p> <p style="padding-left: 40px;">from or at which:</p> <p style="padding-left: 80px;">the Services are (or are to be) provided; or</p> <p style="padding-left: 80px;">the Agency manages, organises or otherwise directs the provision or the use of the Services; or</p> <p style="padding-left: 40px;">where:</p> <p style="padding-left: 80px;">any part of the Agency Information Management System is situated; or</p> <p style="padding-left: 80px;">any physical interface with the Client System takes place.</p>
“Standard Contractual Clauses”	means the standard data protection clauses specified in Article 46 of the United Kingdom General Data Protection Regulation setting out the appropriate safeguards for the transmission of personal data outside the combined territories of the United Kingdom and the European Economic Area.
“Agency Information Management System”	<p>means:</p> <p style="padding-left: 40px;">those parts of the information and communications technology system and the Sites that the Agency or its Sub-contractors will use to provide the Services; and</p>

	the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources);
“Sub-contractor Personnel”	means: any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and engaged in or likely to be engaged in: the performance or management of the Services; or the provision of facilities or services that are necessary for the provision of the Services.
“Agency Personnel”	means any individual engaged, directly or indirectly, or employed by the Agency or any Sub-contractor in the management or performance of the Agency obligations under this Agreement.
“UKAS”	means the United Kingdom Accreditation Service.

4 Introduction

4.1 This Schedule 9 (Security Management) sets out:

- (a) the arrangements the Agency must implement before, and comply with when, providing the Services and performing its other obligations under this Agreement to ensure the security of the Client Data, the Services and the Agency Information Management System;
- (b) the assessment of this Agreement as either a:
 - (i) standard consultancy agreement; or
 - (ii) higher-risk consultancy agreement,
 in paragraph 1;
- (c) the Client's access to the Agency Personnel and Agency Information Management System, in paragraph 6;
- (d) the Certification Requirements, in paragraph 7;
- (e) the requirements for a Security Management Plan in the case of higher-risk consultancy agreements, in paragraph 8; and
- (f) the security requirements with which the Agency and Sub-contractors must comply in Appendix 1.

5 Principles of security

- 5.1** The Agency acknowledges that the Client places great emphasis on the confidentiality, integrity and availability of the Client Data and, consequently on the security of:
- (a) the Sites;
 - (b) the Services; and
 - (c) the Agency's Information Management System.
- 5.2** The Agency is responsible for:
- (a) the security, confidentiality, integrity and availability of the Client Data when that Client Data is under the control of the Agency or any of its Sub-contractors; and
 - (b) the security of the Agency Information Management System.
- 5.3** The Agency:
- (a) comply with the security requirements in Appendix 1; and
 - (b) ensure that each Sub-contractor that Processes Client Data complies with the security requirements in Appendix 1.
- 5.4** Where the Agency, a Sub-contractor or any of the Agency Personnel is granted access to the Client System or to the Client Equipment, it must comply with and ensure that all such Sub-contractors and Agency Personnel comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Client System or the Client Equipment.

6 Access to Agency Personnel and Agency Information Management System

- 6.1** The Client may require, and the Agency must provide the Client and its authorised representatives with:
- (a) access to the Agency Personnel;
 - (b) access to the Agency Information Management System to audit the Agency and its Sub-contractors' compliance with this Agreement; and
 - (c) such other information and/or documentation that the Client or its authorised representatives may reasonably require,
- to assist the Client to establish whether the arrangements which the Agency and its Sub-contractors have implemented in order to ensure the security of the Client Data and the Agency Information Management System are consistent with the representations in the Security Management Plan.
- 6.2** The Agency must provide the access required by the Client in accordance with paragraph 6.1 within ten Working Days of receipt of such request, except in the case of a Breach of Security in which case the Agency shall provide the Client with the access that it requires within 24 hours of receipt of such request.

7 Certification Requirements

- 7.1** The Agency shall ensure that, unless otherwise agreed by the Client, it is certified as compliant with:

- (a) in the case of a standard consultancy agreement the option chosen by the Client in Paragraph 1; or
 - (b) in the case of a higher-risk consultancy agreement:
 - (i) ISO/IEC 27001:2013 by a UKAS-approved certification body in respect of the Agency Information Management System, or the Agency Information Management System is included within the scope of a wider certification of compliance with ISO/IEC 27001:2018; and
 - (ii) Cyber Essentials Plus (“**Relevant Certifications**”).
- 7.2 Unless otherwise agreed by the Client, the Agency must provide the Client with a copy of the Relevant Certifications before it begins to provide the Services.
- 7.3 The Agency must ensure that at the time it begins to provide the Services, the Relevant Certifications are:
- (a) currently in effect;
 - (b) relate to the full scope of the Agency Information System; and
 - (c) are not subject to any condition that may impact the provision of the Services.
- 7.4 The Agency must notify the Client promptly, any in any event within three Working Days of becoming aware that:
- (a) a Relevant Certification has been revoked or cancelled by the body that awarded it;
 - (b) a Relevant Certification expired and has not been renewed by the Agency;
 - (c) a Relevant Certification no longer applies to the full scope of the Agency Information Management System or
 - (d) the body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a “**Certification Default**”).
- 7.5 Where the Agency has notified the Client of a Certification Default under paragraph 7.4:
- (a) the Agency must, within ten working Days of the date in which the Agency provided notice under paragraph 7.4 (or such other period as the Parties may agree) provide a draft plan (a “**Certification Rectification Plan**”) to the Agency setting out:
 - (i) full details of the Certification Default, including a root cause analysis;
 - (ii) the actual and anticipated effects of the Certification Default;
 - (iii) the steps the Agency will take to remedy the Certification Default;
 - (b) the Client must notify the Agency as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;
 - (c) if the Client rejects the Certification Rectification Plan, the Client must within five Working Days of the date of the rejection submit a revised Certification Rectification Plan and paragraph 7.5(b) will apply to the re-submitted plan;
 - (d) the rejection by the Client of a revised Certification Rectification Plan is a material Default of this Agreement;
 - (e) if the Client accepts the Certification Rectification Plan, the Agency must start work immediately on the plan.

8 Security Management Plan

- 8.1** This paragraph 8 applies only where the Client has assessed that this Agreement is a higher-risk consultancy agreement.

Preparation of Security Management Plan

- 8.2** The Agency shall document in the Security Management Plan how the Agency and its Sub-contractors shall comply with the requirements set out in this Schedule 1 (Security Management) and the Agreement in order to ensure the security of the Client Data and the Agency Information Management System.
- 8.3** The Agency shall prepare and submit to the Client within 20 Working Days of the date of this Call-Off Contract, the Security Management Plan, which must include:
- (a)** an assessment of the Agency Information Management System against the requirements of this Schedule 1 (Security Management), including Appendix 1
 - (b)** the process the Agency will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Client Data, the Client, the Services and/or users of the Services; and
 - (c)** the following information in respect of each Sub-contractor:
 - (i)** the Sub-contractor's:
 - (A)** legal name;
 - (B)** trading name (if any);
 - (C)** registration details (where the Sub-contractor is not an individual);
 - (ii)** the Sites used by the Sub-contractor;
 - (iii)** the Client Data Processed by the Sub-contractor;
 - (iv)** the Processing that the Sub-contractor will undertake in respect of the Client Data;
 - (v)** the measures the Sub-contractor has in place to comply with the requirements of this Schedule 1 (Security Management).

- 8.4** The Client shall review the Agency proposed Security Management Plan as soon as possible and must issue the Agency with either:

- (a)** an information security approval statement, which shall confirm that the Agency may use the Agency Information Management System to Process Client Data; or
- (b)** a rejection notice, which shall set out the Client's reasons for rejecting the Security Management Plan.

- 8.5** If the Client rejects the Agency's proposed Security Management Plan, the Agency must prepare a revised Security Management Plan taking the Client's reasons into account, which the Agency must submit to the Client for review within ten Working Days of the date of the rejection, or such other period agreed with the Client.

Updating Security Management Plan

- 8.6** The Agency shall regularly review and update the Security Management Plan, and provide such to the Client, at least once each year and as required by this paragraph.

Monitoring

- 8.7** The Agency shall notify the Client within two Working Days after becoming aware of:
- (a) a significant change to the components or architecture of the Agency Information Management System;
 - (b) a new risk to the components or architecture of the Agency Information Management System;
 - (c) a vulnerability to the components or architecture of the Agency Information Management System using an industry standard vulnerability scoring mechanism;
 - (a) a change in the threat profile;
 - (d) a significant change to any risk component;
 - (e) a significant change in the quantity of Personal Data held within the Service;
 - (f) a proposal to change any of the Sites from which any part of the Services are provided; and/or
 - (g) an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.
- 8.8** Within ten Working Days of such notifying the Clients or such other timescale as may be agreed with the Client, the Agency shall make the necessary changes to the Security Management Plan and submit the updated Security Management Plan to the Client for review and approval.

Appendix 1: Security requirements

1 Location

- 1.1 Unless otherwise agreed with the Client, the Agency must, and must ensure that its Sub-contractors must, at all times, store, access or process Client Data either:
- (a) in the United Kingdom;
 - (b) the European Economic Area; or
 - (c) in a facility operated by an entity where:
 - (i) the entity has entered into a binding agreement with the Agency or Sub-contractor (as applicable);
 - (ii) that binding agreement includes obligations on the entity in relation to security management at least as onerous as those relating to Sub-contractors in this Schedule 9 (Security Management);
 - (iii) the Agency or Sub-contractor has taken reasonable steps to assure itself that
 - (A) the entity complies with the binding agreement;
 - (B) any system operated by the Agency or Sub-contractor has in place appropriate technical and organisational measures to ensure that the Sub-contractor will store, access, manage and/or Process the Government Data as required by this Schedule 1 (*Security Management*); and
 - (iv) the Agency has provided the Client with such information as the Client requires concerning:
 - (A) the entity;
 - (B) the arrangements with the entity; and
 - (C) the entity's compliance with the binding agreement; and
- 1.2 Where the Agency cannot comply with one or more of the requirements of paragraph 1.1:
- (a) it must provide the Client with such information as the Client requests concerning the security controls in places at the relevant location or locations; and
 - (b) the Client may grant approval to use that location or those locations, and that approval may include conditions; and
 - (c) if the Client does not grant permission to use that location or those locations, the Agency must cease to store, access or process Client Data at that location or those locations within such period as the Client may specify.
- 1.3 The Client may by notice in writing at any time give notice to the Agency that it and its Sub-contractors must not undertake or permit to be undertaken, the storage, access or Processing Client Data as specified in the notice (a "**Prohibited Activity**").
- (a) in any particular country or group of countries;
 - (b) in or using facilities operated by any particular entity or group of entities; or

- (c) in or using any particular facility or group of facilities, whether operated by the Agency, a Sub-contractor or a third-party entity (a “**Prohibition Notice**”).

1.4 Where the Agency or Sub-contractor, on the date of the Prohibition Notice undertakes any Relevant Activities affected by the notice, the Agency must, and must procure that Sub-contractors, cease to undertake that Prohibited Activity within 40 Working Days of the date of the Prohibition Notice.

2 **Vetting, Training and Staff Access**

Vetting before performing or managing Services

2.1 The Agency must not engage Agency Personnel, and must ensure that Sub-contractors do not engage Sub-contractor Personnel, in any activity relating to the performance and management of the Services unless:

- (a) That individual has passed the security checks listed in paragraph 2.2; or
- (b) The Client has given prior written permission for a named individual to perform a specific role.

2.2 For the purposes of paragraph 2.1, the security checks are:

- (a) the checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:
 - (i) the individual's identity;
 - (ii) the individual's nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;
 - (iii) the individual's previous employment history; and
 - (iv) that the individual has no Relevant Convictions;
- (b) national security vetting clearance to the level specified by the Client for such individuals or such roles as the Client may specify; or
- (c) such other checks for the Agency Personnel of Sub-contractors as the Client may specify.

Annual training

2.3 The Agency must ensure, and ensure that Sub-contractors ensure, that all Agency Personnel, complete and pass security training at least once every calendar year that covers:

- (a) general training concerning security and data handling; and
- (b) phishing, including the dangers from ransomware and other malware.

Staff access

2.4 The Agency must ensure, and ensure that Sub-contractors ensure, that individual Agency Personnel can access only the Client Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.

2.5 The Agency must ensure, and ensure that Sub-contractors ensure, that where individual Agency Personnel no longer require access to the Client Data or any part of the Client Data, their access to the Client Data or that part of the Client Data is revoked immediately when their requirement to access Client Data ceases.

- 2.6 Where requested by the Client, the Agency must remove, and must ensure that Sub-contractors remove, an individual Agency Personnel's access to the Client Data or part of that Client Data specified by the Client as soon as practicable and in any event within 24 hours of the request.

Exception for certain Sub-contractors

- 2.7 Where the Agency considers it cannot ensure that a Sub-contractors will undertake the relevant security checks on any Sub-contractor Personnel, it must:
- (a) as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Client;
 - (b) provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Agency Personnel will perform as the Client reasonably requires; and
 - (c) comply, at the Agency cost, with all directions the Client may provide concerning the vetting of the affected Sub-contractor Personnel and the management of the Sub-contractor.

3 Security Testing

- 3.1 This paragraph applies only where the Client has assessed that this Agreement is a higher-risk consultancy agreement.

Note: the definition of Agency Information Management System includes those information and communications technology systems that Sub-contractors will use to assist or contribute to the Agency providing the Services.

- 3.2 The Agency must, at the Client's option, before providing the Services and when reasonably requested by the Client, either:
- (a) conduct security testing of the Agency Information Management System by:
 - (i) engaging a CHECK Service Provider or a CREST Service Provider;
 - (ii) designing and implementing the testing so as to minimise its impact on the Agency Information Management System and the delivery of the Services; and
 - (iii) providing the Client with a full, unedited and unredacted copy of the testing report without delay and in any event within ten Working Days of its receipt by the Agency; or
 - (b) Provide details of any security testing undertaken by a CHECK Service Provider or a CREST Service Provider in respect of the Agency Information Management System in the calendar year immediately preceding the Client's request or the Effective Date (as appropriate), including:
 - (i) the parts of the Agency Information Management System tested;
 - (ii) a full, unedited and unredacted copy of the testing report; and
 - (iii) the remediation plan prepared by the Agency to address any vulnerabilities disclosed by the security testing; and
 - (iv) the Agency progress in implementing that remediation plan.
- 3.3 The Agency must remediate any vulnerabilities classified as "medium" or above in the security testing:

- (a) before Processing Client data where the vulnerability is discovered before the Agency begins to process Authority Data;
- (b) where the vulnerability is discovered when the Agency has begun to Client Data:
 - (i) by the date agreed with the Client; or
 - (ii) where no such agreement is reached:
 - (A) within five Working Days of becoming aware of the vulnerability and its classification where the vulnerability is classified as critical;
 - (B) within one month of becoming aware of the vulnerability and its classification where the vulnerability is classified as high; and
 - (C) within three months of becoming aware of the vulnerability and its classification where the vulnerability is classified as medium.

4 End-user Devices

- 4.1 The Agency must manage, and must ensure that all Sub-contractors manage, all End-user Devices on which Client Data is stored or processed in accordance the following requirements:
- (a) the operating system and any applications that store, process or have access to Client Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;
 - (b) users must authenticate before gaining access;
 - (c) all Client Data must be encrypted using a encryption tool agreed to by the Client;
 - (d) the End-user Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;
 - (e) the End-user Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Client Data;
 - (f) the Agency or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Client Data on the device and prevent any user or group of users from accessing the device;
 - (g) all End-user Devices are within in the scope of any current Cyber Essentials Plus certificate held by the Agency, or any ISO/IEC 27001:2018 certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.
- 4.2 The Agency must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Agreement.
- 4.3 Where there any conflict between the requirements of this Schedule 9 (Security Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.

5 Encryption

- 5.1 Unless paragraph 5.2 applies, the Agency must ensure, and must ensure that all Sub-contractors ensure, that Client Data is encrypted:
- (a) when stored at any time when no operation is being performed on it; and
 - (b) when transmitted.
- 5.2 Where the Agency, or a Sub-contractor, cannot encrypt Client Data as required by paragraph 5.1, the Agency must:
- (a) immediately inform the Client of the subset or subsets of Client Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
 - (b) provide details of the protective measures the Agency or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Client as encryption;
 - (c) provide the Client with such information relating to the Client Data concerned, the reasons why that Client Data cannot be encrypted and the proposed protective measures as the Client may require.
- 5.3 The Client, the Agency and, where the Client requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Client Data.
- 5.4 This paragraph applies where the Client has assessed that this Agreement is a higher-risk consultancy agreement.
- Where the Client and Agency reach agreement, the Agency must update the Security Management Plan to include:
- (a) the subset or subsets of Client Data not encrypted and the circumstances in which that will occur;
 - (b) the protective measure that the Agency and/or Sub-contractor will put in place in respect of the unencrypted Client Data.
- 5.5 Where the Client and Agency do not reach agreement within 40 Working Days of the date on which the Agency first notified the Client that it could not encrypt certain Client Data, either party may refer the matter to be determined by an expert in accordance with the Dispute Resolution Procedure.

6 Access Control

- 6.1 The Agency must, and must ensure that all Sub-contractors:
- (a) identify and authenticate all persons who access the Agency Information Management System and Sites before they do so;
 - (b) require multi-factor authentication for all user accounts that have access to Client Data or that are Privileged Users;
 - (c) allow access only to those parts of the Agency Information Management System and Sites that those persons require;
 - (d) maintain records detailing each person's access to the Agency Information Management System and Sites, and make those records available to the Client on request.
- 6.2 The Agency must ensure, and must ensure that all Sub-contractors ensure, that the user accounts for Privileged Users of the Agency Information Management System:

- (a) are accessible only from dedicated End-user Devices;
 - (b) are configured so that those accounts can only be used for system administration tasks;
 - (c) require passwords with high complexity that are changed regularly;
 - (d) automatically log the user out of the Agency Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive.
- 6.3 The Agency must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different passwords for their different accounts on the Agency Information Management System.
- 6.4 The Agency must, and must ensure that all Sub-contractors:
- (a) configure any hardware that forms part of the Agency Information Management System that is capable of requiring a password before it is accessed to require a password; and
 - (b) change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.

7 Malicious Software

- 7.1 The Agency shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Agency Information Management System.
- 7.2 The Agency shall ensure that such Anti-virus Software:
- (a) is configured to perform automatic software and definition updates;
 - (b) performs regular scans of the Agency Information Management System to check for and prevent the introduction of Malicious Software; and
 - (c) where Malicious Software has been introduced into the Agency Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.
- 7.3 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Client Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.
- 7.4 Any cost arising out of the actions of the parties taken in compliance with the provisions of paragraph 7.3 shall be borne by the parties as follows:
- (a) by the Agency where the Malicious Software originates from the Agency Software, any third-party software licenced by the Agency or the Client Data (whilst the Client Data was under the control of the Agency) unless the Agency can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Agency when provided to the Client; and
 - (b) by the Client, in any other circumstance.

8 Breach of Security

- 8.1 If either party becomes aware of a Breach of Security it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within 24 hours.

- 8.2 The Agency must, upon becoming aware of a Breach of Security or attempted Breach of Security immediately take those steps identified in the Security Management Plan (if applicable) and all other reasonably steps necessary to:
- (a) minimise the extent of actual or potential harm caused by such Breach of Security;
 - (b) remedy such Breach of Security to the extent possible;
 - (c) apply a tested mitigation against any such Breach of Security; and
 - (d) prevent a further Breach of Security in the future which exploits the same root cause failure.
- 8.3 As soon as reasonably practicable and, in any event, within five Working Days, or such other period agreed with the Client, following the Breach of Security or attempted Breach of Security, provide to the Client full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Client.
- 8.4 The Agency must take the steps required by paragraph 8.2 at its own cost and expense.

9 **Sub-contractors**

The Agency must assess the parts of the information and communications technology system and the Sites that its Sub-contractors will use to provide the Services against the NCSC Cloud Security Principles at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-contractor must document that assessment and make that documentation available to the Client at the Client request.

10 **Third-party Software**

The Agency must not, and must ensure that Sub-contractors do not, use any software to Process Client Data where the licence terms of that software purport to grant the licensor rights to Progress the Client Data greater than those rights strictly necessary for the use of the software.

11 **Deletion of Client Data**

The Agency must, and must ensure that all Sub-contractors, securely erase any or all Client Data held by the Agency or Sub-contractor when requested to do so by the Client using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.