[redacted]

Crown Commercial Service

Call Off Order Form for Public Sector Resourcing Model Services ("Call Off Order Form")

FINAL 24/01/2020

[redacted]

PUBLIC SECTOR RESOURCING CALL OFF ORDER FORM AND PUBLIC SECTOR RESOURCING CALL OFF TERMS

PART 1 – PUBLIC SECTOR RESOURCING 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 Public Sector Resourcing Model Services dated 16 January 2018 between Crown Commercial Service and the Service Provider (as defined below) (the "**Framework Agreement**").

The Call Off Contract, referred to throughout this Call Off Order Form, means the contract between the Service Provider and the Customer (entered into pursuant to the terms of the Framework Agreement) consisting of this Call Off Order Form and the Call-off Contract.

In this Call Off Order Form, capitalised expressions shall have the meanings set out in Schedule 1 (Definitions) to the Call-off Contract, Schedule 1 to the Framework Agreement or the relevant Appendix to this Call Off Order Form in which that capitalised expression appears.

The Service Provider agrees to supply the Services specified in this Call Off Order Form (including any Appendices to this Call Off Order Form) to the Customer on and subject to the terms of this Call Off Contract, and for the duration of the term of the Call Off Contract.

In the event of and to the extent only of a conflict between any of the provisions of the Framework Agreement, the Call Off Contract, and the Call Off Order Form, the conflict shall be resolved, in accordance with clause 1.4 of the Call Off Contract.

This Call Off Order Form shall comprise the following:

- this document headed "Call Off Order Form for Public Sector Resourcing Model Services ("Call Off Order Form")";
- Appendix 1 – Requisition Process;
- Appendix 2 – Issue Resolution and Escalation Management;
- Appendix 3 –MI Dashboard;
- Appendix 4 – Revised KPIs;
- [redacted]
- Appendix 6 – Standard Contractual Clauses;
- Appendix 7 – NHS Digital Security Policy;
- Appendix 8 – NHS Digital ICT Policy;
- [redacted]
- Appendix 10 – Business Continuity and Disaster Recovery;
- [redacted] and
- Appendix 12 – Customer's IR35 Process.

From	**Health and Social Care Information Centre ("NHS Digital"), of 1 Trevelyan Square, Boar Lane, Leeds , West Yorkshire LS1 6AE ("CUSTOMER")** [redacted]

[redacted]

	("CUSTOMER REPRESENTATIVE")
To	**Alexander Mann Solutions Limited (Company number 02073305) of 7 Bishopsgate, London, EC2N 3AQ** **("SERVICE PROVIDER")** [redacted] **("SERVICE PROVIDER REPRESENTATIVE")**

The Customer and the Service Provider shall each be referred to as a "**Party**" and together be referred to as the "**Parties**".

SECTION B

1	**Definitions**
1.1	The following new definitions shall be added to Schedule 1 (Definitions) of the Call Off Contract: • "**Elevate Direct**" or "**Elevate Platform Limited**" means the self-service technology platform which the Customer can use to advertise its own contingent labour requirements and recruit contractors directly. The Customer will then pass the identified Workers to the Service Provider to onboard in accordance with the Call Off Contract. • "**Intellirate**" means a proprietary tool (or any similar tool created by an alternative provider at the sole discretion of the Service Provider). • "**Contract Charges Schedule**" means Annex 1 (Call Off Contract Charges) to Schedule 3 (Call Off Contract Charges, Payment and Invoicing), to be revised as set out in the Framework Agreement, and subject to section 6.1 of the Order Form in relation to this Call Off Contract only. • "**Fieldglass**" means a SAP cloud-based VMS (Vendor Management System) software platform, that allows the Customer to manage the end-to-end process of obtaining and managing Workers. • "**Migration**" means the process whereby Worker(s) engaged by the Customer through a staffing company/agency outside of the Framework Agreement, leaving the engagement of their respective staffing company/agency to be directly engaged by the Service Provider under the Framework Agreement and provided to the Customer. [redacted]

	• "**Services Schedule**" means Schedule 2 (Services) to the Call Off Terms, excluding paragraph 9.3.4 of Annex 1. • "**Transition**" means the process whereby the staffing company/agency engaged by the Customer to provide contingent workers outside of the Framework Agreement, terminates its direct engagement with the Customer, and: o signs up to the Framework Agreement as an Agency Provider and is brought within the PSR supply chain; and o the staffing company/agency provider (including all Workers engaged by the Customer), are contracted via the Framework Agreement. The following definitions shall be revised for the purposes of this Call Off Contract: • **"Call Off Contract Charges"** shall mean the charges set out in the Contract Charges Schedule.

2	**CALL OFF CONTRACT PERIOD**
2.1	**Term**: The term of this Call Off Contract shall be from 27th January 2020 ("**the Service Commencement Date**") until the expiry of the Framework Agreement on 17/1/2024 ("**Call Off Initial Period**"). The Customer intends to make use of the option to extend for a further 18 months after the expiry of the Framework Agreement. However, this shall specifically be requested by the Customer giving a minimum of 30 days prior written notice, under Clause 5.2 of the Call Off Terms ("**Call Off Extension Period**") prior to the end of the Call Off Initial Period.
2.2	**Non Exclusivity:** For the avoidance of doubt, and in accordance with Clause 4.2 of the Framework Agreement: • there is no obligation whatsoever on the Customer to use the Service Provider to provide any Services and/or to purchase any Services under this Call Off Contract; and • in entering into this Call Off Contract no form of exclusivity has been conferred on the Service Provider, nor volume or value guarantee granted by the Customer in relation to the provision of the Services by the Service Provider, and that the Customer is at all times entitled to enter into other contracts and agreements with other service providers for the provision of any or all services which are the same as or similar to the Services.

3	**SERVICES**
3.1	**Services** – The Service Provider shall provide the services as specified in Annex 1 (The Services) to Schedule 2 (Services) of the Call Off Terms, and as further set out herein. The Service Provider shall give the Customer access to Intellirate. The Customer shall within two (2) weeks of the Service Commencement Date be provided with [redacted] logins to

[redacted]

	the commercial function who hold responsibility for the management of the Customer's contingent spend which will allow it to access Intellirate. **Requisitions** - The Service Provider's procedure for requisitions is set out in Appendix 1. **Transition and Migration** - The Service Provider shall provide Transition and Migration services as further set out in the Phase 1 and Phase 2 Implementation Plans (as updated and agreed) **Health Workers** - Whilst the Customer may seek to engage "NHS/Health Workers" for their qualifications experience and expertise of their function, this would not be for the purposes of 'healthcare services', since the Customer is not a provider of healthcare services (as defined in legislation). For the avoidance of doubt, the onboarding and security vetting as set out in paragraph 9.3.4 of the Services Schedule shall not apply. The Service Provider shall provide a nominated Client Services Manager at the Service Commencement Date to act as the first point of contact for all issues relating to the Services and this Call Off Contract. The account support shall be reviewed by the Parties after 6 months and (provided that a minimum of 50 or more Professional Interims (as defined in 3.2.1 of the Services Schedule) are supplied by the Service Provider and have commenced work for the Customer, then the Service Provider shall continue to provide a nominated Client Services Manager. If the volume of Workers is less than this, then the Service Provider shall provide a nominated Account Specialist instead of a Client Services Manager.
3.2	**Continuous Improvement** The Service Provider shall report progress on continuous improvement (as set out in the Services Schedule). The Parties will work together to identify improvement opportunities through the action log and account management framework and the Service Provider shall raise any agreed improvement opportunities with the Authority in accordance with Clause 13 of the Services Schedule.

[redacted]

[redacted]

[redacted]

5	CONTRACT PERFORMANCE
5.1	**Standards:** The following provisions shall be added to Clause 11 (Standards and Quality) of the Call Off Contract: (a) The Service Provider shall comply with and be certified to Cyber Essentials Plus. (b) The Service Provider shall hold certification to ISO 27001, and shall provide a statement of applicability for all elements of the Service. (c) The Service Provider shall hold certification to ISO 9001:2008.
5.2	**Conflict of Interest** In the event that the Customer reasonably believes there to have been a conflict of interest under Clause 8.7 of the Call Off Contract, it shall notify the Service Provider promptly and the Service Provider shall investigate the matter and respond in accordance with the Issue Resolution and Escalation Management procedure attached at Appendix 2 to this Call Off Order Form.
5.3	**KPI's** Variation of Schedule: The KPIs set out in Schedule 18 of the Call Off Terms shall cease to have effect, and shall be replaced by the Revised KPIs as set out in Appendix 4 to the Call Off Order Form (and the definition of 'KPIs' shall be interpreted as meaning those set out in Appendix 4 of the Call Off Order Form (as amended)). The KPIs shall remain under review, and shall be updated following agreement with the Authority in accordance with the KPI amendments under the Framework Agreement.

5.4	**Period for providing Rectification Plan:** As per Clause 38.2.1(a) of the Call Off Terms.

6	**PAYMENT**
6.1	**Call Off Contract Charges** (including any applicable discount(s), but excluding VAT): The Call Off Contract Charges are varied as set out in Appendix 12 (Variation of Charges). [redacted]
6.2	**Electronic Invoicing** Clause 23.6.1 (Option 1) shall not apply to this Call Off Contract. Clauses 23.6.2 and 23.6.3 (Option 2) shall apply to this Call Off Contract, and the Parties shall consider the invoicing approach as part of the Implementation Plan.
6.3	**Payment terms/profile** (including method of payment e.g. Government Procurement Card (GPC) or BACS): The following is a clarification of the applicable payment terms: Payments under the Call Off Contract shall be made by the Customer in accordance with the terms of the Procurement Policy Note 05/15 (prompt payment policy and performance of reporting). The Service Provider will invoice the Customer each week in arrears following the drawdown of approved timesheets from the VMS or other appropriate collation of approved manual timesheets (as the case may be).
6.4	**Temp to Temp Transfer Fees** For the avoidance of doubt, on expiry of the Framework Agreement or terminations in accordance with Clauses 41, 42, 43 or 44 of the Call Off Terms, the Temp to Temp transfer fee described contained in the Contract Charges Schedule shall not apply to any Non-Agency Supply Workers provided by the Service Provider to a Replacement Service Provider. Where a Non-Agency Supply Worker has been sourced directly by the Service Provider, they will be transitioned to the Replacement Service Provider under an agency agreement.
6.5	[redacted]
6.6	

6.7	**Pre-Identified Workers and Nominated Worker** 6.7.1 For the purpose of the Call Off Contract, a pre-identified, referred or Nominated Worker (together **"Nominated Worker"**) is a Worker that has: • been identified by the Customer, through its internal talent management processes, referral or recommendation, as having the skills and experience which meet the requirements for a role that that the Customer has raised in Fieldglass; and • the Customer has asked the Service Provider to onboard as a Worker under the terms of the Call Off Contract. 6.7.2 For the avoidance of doubt, a Worker that has previously been supplied to the Customer by an Agency Provider under the PSR framework cannot be a Nominated Worker until twenty six (26) weeks have elapsed since the commencement of their last assignment for the Customer, where the Agency Provider supplied the Worker. 6.7.3 For the avoidance of doubt, subject to 6.7.2, where prior to Customer's nomination, the Service Provider has given the Worker name in response to a Customer request then such Worker shall not be classed a Nominated Worker.
6.8	**Customer billing address** (paragraph 7.6 of Call Off Schedule 3 (Call Off Contract Charges, Payment and Invoicing). HSCIC T56 Payables A125 Phoenix House, Topcliffe Lane Wakefield West Yorkshire WF3 1WE With a copy and back up sent to: nhsdigital.payroll@nhs.net NHS Digital 1 Trevelyan Square Boar Lane Leeds West Yorkshire LS1 6AE

7	**LIABILITY AND INSURANCE**
7.1	**Estimated Year 1 Call Off Contract Charges**: The sum of £4,000,000 (four million pounds)
7.2	**Service Provider's limitation of Liability** As per Clause 36.2.1 of the Call Off Terms.

8	**TERMINATION AND EXIT**

8.1	**Termination on material Default** As per Clause 41.2.1(c) of the Call Off Terms
8.2	**Termination without cause notice period** As per Clause 41.7.1 of the Call Off Terms
8.3	**Undisputed Sums Limit**: As per Clause 42.1.1 of the Call Off Terms
8.4	**Exit Management:** Notwithstanding Call Off Schedule 9 (Exit Management), an initial Exit Plan ("Exit Plan") has been agreed with the Authority and is available from the Authority, on demand. Within 4 weeks of the Service Commencement Date, the Customer will develop a draft schedule to the Exit Plan to identify any reasonable Contracting Authority exit requirements should either Party terminate the Call Off Contract for any reason ("Exit Plan Schedule"). The Parties shall discuss the Exit Plan Schedule and agree a final version as part of Implementation (and no later than 6 months of the Service Commencement Date).

9	**OTHER CALL OFF REQUIREMENTS**
9.1	**Compliance** The Service Provider shall inform Workers (and for the avoidance of doubt, any other personnel who have access to the Customer's Premises pursuant to authority provided by the Service Provider) that, while on the Customer's Premises, they are required to adhere to the following: (a) all applicable laws, statutes, regulations in force from time to time; and (b) the NHS Digital mandatory policies, (together the "**Mandatory Requirements**") The NHS Digital mandatory policies will be provided to the Worker by the Customer as part of the induction training provided by the Customer. The Customer shall be entitled to remove or to refuse admission to any Worker who is, or has been, in breach of NHS Digital's Mandatory Requirements. The Customer shall advise the Worker of the applicable NHS Digital mandatory policies that apply from time to time. For information, NHS Digital mandatory policies are likely to include coverage of the following topics: • Modern Slavery and Human Trafficking; • Anti-bribery and Anti-corruption; • Data and Privacy; • Personnel Security and Vetting; • Health and Safety; • ICT working practices; • Information and Governance & Reporting. • IPR Policy Upon request by the Customer, the Service Provider shall promptly provide to the Customer evidence that it has notified the Worker that they are obliged to comply with the NHS Digital mandatory policies as part of the onboarding pack.
9.2	**Business Continuity & Disaster Recovery**:

[redacted]

	As per Schedule 8 (Business Continuity and Disaster Recovery) of the Call Off Contract, the Business Continuity and Disaster Recovery Plan is attached at Appendix 10 to the Call Off Order Form. **Disaster Period**: For the purpose of the definition of "Disaster" in Call Off Schedule 1 (Definitions) the "Disaster Period" shall be one calendar month.
9.3	**Notices** Customer's postal address and email address: Commercial Department 1 Trevelyan Square, Boar Lane, Leeds, West Yorkshire, LS1 6AE Email: nhsdcommercial@nhs.net Copied to legal.team@nhs.net Service Provider's postal address and email address: 7-11 Bishopsgate, London, EC2N 3AQ Email: [redacted]
9.4	**Corporate Social Responsibility Conduct and Compliance** The Customer applies corporate and social responsibility values to its business operations and activities which are consistent with the Government's corporate social responsibility policies, including, without limitation, those policies relating to anti-bribery and corruption, health and safety, the environment and sustainable development, equality and diversity. The Service Provider shall, on request, share its corporate social responsibility policy with the Customer.
9.5	**Modern Slavery** The Service Provider shall, on request, share its modern-day anti-slavery policy with the Customer. The Service Provider shall procure by contract that its Sub-Contractors are complying with applicable Laws, which, by definition, include those related to slavery and human trafficking.
9.6	**Exception to the PSR process** 9.6.1 Where the Customer reasonably believes that they have a requirement that needs to be filled on an urgent basis, or requires a niche skillset, the Customer Representative may request an exception to the standard PSR process whereby the Service Provider distributes the Worker requirement directly to Agency Providers. 9.6.2 The Service Provider shall use reasonable endeavours to engage the Agency Provider under the Framework Agreement on its standard rates. Where this is not possible, the Service Provider shall first advise the Customer of the issue and the additional cost. If the Customer agrees to proceed, the additional Agency Provider cost and applicable Service Provider uplifts as set out in the Charges as advised by the Service Provider, shall be met by the Customer. 9.6.3 In the event that the Service Provider is unable to provide CVs for a role within 15 Working Days, it will use commercially reasonable endeavours to bring the Agency Provider

	recommended by the Customer within the Framework Agreement, provided the Agency Provider passes the Service Provider's onboarding checks and agrees to the Service Provider's terms of business. 9.6.4 The Parties shall meet on a quarterly basis to review the use of exceptions to the PSR process and in good faith, seek to reach agreement regarding how such exceptions will be managed in the following quarter, in line with the aims of the Framework Agreement and Good Industry Practice. Where the number of exceptions to the PSR process under 9.6.1 above result in an increased administrative burden on the Service Provider, the Service Provider shall notify the Customer and advise the Customer of the additional costs associated with the additional administrative burden (together with evidence of the same). The Parties accept that if the Customer wishes to continue with the same level of exceptions the Service Provider may charge the Customer for any reasonable administrative costs associated with any subsequent exceptions.
9.7	**International Data Transfers** In the event that the UK leaves the European Union and where: (i) no adequacy decision has been made by the European Commission concerning the UK under Article 45 of the GDPR; and (ii) the UK is not subject to a legal transition period under which it is treated by the European Union as a Member State for the purposes of European Union law (such as the one created by Article 126 of the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, as endorsed by leaders at a special meeting of the European Council on 25 November 2018), the Parties agree, to the extent they are both acting as Controllers: • to enter into the Standard Contract Clauses set out in the attached Appendix 6 to Call-Off Order Form in respect of data transfers by the Service Provider outside of the EEA; and • the following new definition shall be introduced into Schedule 1 – Definitions of the Call Off Terms: "**Standard Contractual Clauses**" means the standard data protection clauses adopted by the European Commission under Article 46(2)(c) of the GDPR (and which remain valid under the GDPR pursuant to Article 46(5) of the GDPR), in relation to the transfer of Personal Data from a Controller established in the EEA to a Controller established in a third country. To the extent the Service Provider is acting as a Processor on behalf of the Customer, the UK Government has stated that, on the UK's exit from the EU, transfers of Personal Data from the UK to the European Economic Area ("EEA") will be permitted. In the event that (i) the transfer of Personal Data from an EEA based Processor to a UK-based Controller is deemed by the European Commission to be a 'restricted transfer' under the GDPR; and (ii) such a transfer is a possibility under the Call Off Contract; and (iii) the European Commission issues standard contractual clauses for such transfers, on request by the Customer the Service Provider agrees to promptly execute the change to incorporate such standard contractual clauses, and perform such acts as may be reasonably be required for the purpose of giving full effect to the Call Off Contract.
9.8	**Data Protection**

	The Parties acknowledged that notwithstanding the terms of the Call Off Contract and the Framework Agreement, further work is required to determine how a data incident is managed and to finalise the DPIA. The Parties will develop an incident management plan with the Authority which sets out how a data breach will be managed across the Framework. The Parties agree that in the event of a possible Personal Data Breach involving the Services, each will inform the other at the earliest opportunity, but in any event within 3 days of discovery. The Service Provider shall be responsible for investigating its systems and operations to identify the causes, evidence and impacts of the Personal Data Breach and informing the Customer (in relation to any breach impacting its Workers).
9.9	**Worker Substitution** The Service Provider will inform a Worker that where they seek to nominate a substitute, the Worker is required at its own cost to ensure: • such a substitute shall first be required to complete any necessary onboarding. Until such time as the substitute has completed such onboarding in accordance with paragraph 9.3.1 of the Services Schedule, such substitutes shall not be permitted access to Customer workplace and systems; • such a substitute shall also be required to first meet the Mandatory Requirements, as required of the existing Worker (it is estimated that this will take up to 3 days). The Customer shall ensure that its substitution process is documented in the Mandatory Requirements.
9.10	**IR35 Determination** For new Workers, and for existing Workers transitioned or migrated over, the Customer will assess whether the Worker Services are in or out of the scope of IR35, and the Customer will inform the Worker accordingly. At a minimum the Customer will ensure that the Worker is assessed in accordance with the Government CEST procedure. The Customer also has additional detailed assessment requirements as documented in the NHS Digital IR35 Assessment Procedure (as updated from time to time), the current version is set out in Appendix 12 (Customer's IR35 Process). The Service Provider shall inform the Worker of the Customer's requirements and that there is a cost to be met by the Worker (details to be advised by the Customer). Should either process result in an assessment that the Worker is inside of IR35, then the Worker shall be treated as inside of scope of IR35 in accordance with the Service Provider's standard processes for managing in scope workers. The Parties will develop a mechanism for handling the payment of out of scope workers using Milestone Payments as part of the work that the Service Provider is doing with the Authority to develop a SOW category. Until such time as this mechanism is agreed and implemented, the Customer accepts that if it asks the Service Provider to migrate or onboard a new Worker that it has assessed as out of scope of IR35, then notwithstanding

	the NHS Digital IR35 Assessment Procedure set out at Appendix 12, the Service Provider will onboard and contract with the Worker in accordance with its standard processes for managing out of scope workers. The Service Provider shall provide any information reasonably requested and available to the Service Provider and facilitate contact between the Customer and the Worker to enable the completion of the assessments. The Customer shall continue to review the role scope, and whether the role remains in or outside of scope of IR35. In the event that the Customer determines that the role's status changes at any time then it will inform the Worker and the Service Provider as soon as reasonably practicable and the Service Provider will amend the Worker's contract. For the avoidance of doubt there will be no cost to the Customer if a Worker's contract is amended at the extension of an Assignment. Any contract changes made as a result of an IR35 status change during the period of an Assignment will be at the Customer's cost.
9.11	**IR35 Indemnity** 9.11.1 - Clauses 9.11.2 to 9.11.3 shall not apply where the Customer has determined a Worker is on payroll (inside of IR35), and communicated this to the Service Provider. 9.11.2 – The Customer is a public sector entity. It is recognised that whilst the Service Provider will be gathering the Worker's information, the Service Provider will then rely on the performance by the Customer of its assessment of the Worker's off payroll status in accordance with HMRC guidance (as applicable from time to time). 9.11.3 – Subject to the Service Provider's compliance with clause 9.11.4, and subject to the limitation of its liability under clause 9.11.5, the Customer shall indemnify the Service Provider on a continuing basis in relation to any claim by the HMRC against the Service Provider for any additional taxes or additional national insurance contributions, in relation to the Workers provided by the Service Provider pursuant to this Call Off Contract that have been classified as off payroll (out of scope of IR35) by the Customer due to a failure of the Customer to undertake the IR35 assessment with reasonable skill and care in accordance with HMRC guidance (the "Claim"). For the avoidance of doubt, this indemnity shall also include any external legal fees, reasonably necessarily incurred by the Service Provider as a result of the aforementioned Claim by HMRC, provided that such aforementioned Claim relates to Customer staff only. If the aforementioned Claim also relates to other Customers, then the Customer shall only be responsible for a reasonable pro rata proportion based on the number of Workers within the scope of the Claim. 9.11.4 - Where the Service Provider wishes to exercise this clause (i) it shall first notify the Customer of the issue providing details of the failure, and (ii) shall permit the Customer to have conduct and to respond to such claim from the HMRC, and (iii) shall also provide any requested information and assistance in relation to the development of any such response. 9.11.5 - The liability of the Customer in accordance with this clause 9.11 shall not exceed (i) the sum of two million (£2,000,000) pounds per claim by the Service Provider, and (ii) the sum of ten million (£10,000,000) pounds in aggregate under the terms of this Call Off Contract."

9.12	**Transfer of Undertakings (Protection of Employment Regulations) 2006 ("TUPE")** The Service Provider will not create an organised grouping of staff that are dedicated to delivering Services to the Customer
9.13	**Milestone Payments** In the event that during the term of the Call Off Contract there becomes available, an option, via the Service Provider, for the Customer to pay the Call Off Contract Charges via milestone payments, the Service Provider agrees that it shall promptly provide the Customer with notice of such development.
9.14	**Brexit Statement.** To the extent applicable, the Parties agree they shall provide reasonable assistance to each other, to mitigate the impact of Brexit, in whatever form it may take, in relation to the provision of the Services.
9.15	**Execution and Counterparts** This Call Off Contract may be executed in any number of counterparts (including by electronic transmission), each of which when executed shall constitute an original but all counterparts together shall constitute one and the same instrument. Execution of this Call Off Contract may be carried out in accordance with the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (SI 2016/696) and the Electronic Communications Act 2000. In the event each Party agrees to sign this Call Off Contract by electronic signature (whatever form the electronic signature takes) it is confirmed that this method of signature is as conclusive of each Party's intention to be bound by this Call Off Contract as if signed by each Party's manuscript signature. In such situation, this Call Off Contract shall be formed on the date on which both Parties have electronically signed the Call Off Contract as recorded in NHS Digital's electronic contract management system.

FORMATION OF CALL OFF CONTRACT

BY SIGNING AND RETURNING THIS CALL OFF ORDER FORM (which may be done by electronic means) the Service Provider agrees to enter a Call Off Contract with the Customer to provide the Services in accordance with the 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 Framework Agreement 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 Service Provider within two (2) Working Days from such receipt.

[redacted]

For and on behalf of the Service Provider:

For and on behalf of the Customer:

[redacted]

Appendix 1

Requisition Process

[redacted]

Appendix 2

Public Sector Resourcing Issue Resolution and Escalation Management

Appendix 2 PSR Issue Resolution.docx

Public Sector Resourcing Issue Resolution and Escalation Management

Escalation - Our service aim will be to ensure that complaints and issues are minimised throughout the delivery of our service, and managed within the framework of the Joint Governance Structure (JGS). Our issue management and escalation process will be documented within our issue management and escalation plan and form part of our bespoke PSR Governance Manual developed during Service Mobilisation. It will also form a critical part of the training for all AMS employees. We will collectively agree with the Authority the classification criteria for Tier 1, 2 and 3 of Operational and Executive escalations.

Operational Escalation: Issues/escalations will be documented within the relevant Issues Log, indicating the type of escalation, and the Account Managers/Deputy Framework Managers notified. The Account Manager will make an initial assessment of the issue and allocate an appropriate level of severity to Tier 1, 2 or 3:

Tier 1 – Account Manager: Includes incidents that have minimal impact on the service and cause no disruption to normal service operation, (as designated by the Authority) can be closed out by the Account Manager. At this point the issue would normally be resolved however if it remains unresolved in 24 hours it moves to Tier 2.

Tier 2 – Deputy Framework Manager: If the issue remains unresolved in a further 48 hours (cumulative 72 hours), the Deputy Framework Manager will investigate the issue in-conjunction with the Account Manager, closing the issue once resolved. We will develop a grading system to ensure immediate escalation if the issue is deemed to be serious/requires escalation.

Tier 3 – Framework Director: If the issue remains unresolved in a further 36 hours (cumulative 108 hours) or the initial issue is identified as an incident that has a severe impact on the reputation or delivery of the Service then an immediate Tier 3 rating is given and the Framework Director must own/close the issue. The resolution of a Tier 3, led by the Framework Director will involve a skilled team to investigate, identify root cause, develop recommendations/appropriate plans to resolve, and document fully. All findings and recommendations will be presented to the agreed JGS authority for sign off. The Deputy Framework Manager will own the fix and communication of resolution to all impacted parties.

Executive Escalation - Issues will be tabled to the Executive Board presented by the AMS MD for Public Sector when they are indicative of a trend or significant reputational risk, not for their transactional resolution which will have occurred at Tier 3 operational level but to enable proactive preventative measures to be identified and taken.

[redacted]

Appendix 3

MI Dashboard [redacted]

Appendix 4

Revised KPIs

Appendix 4a KPIs Professional Workers.

Appendix 4b KPI's Admin & Clerical.pptx

Service KPI's

KPI	Description	Measurement
Time to shortlist	Time from Approved requirement to 2nd CV sent to HM within 3 Business Days for all roles closed in the previous month	85%
CV to Interview	Number of CVs submitted for each interview arranged	3 to 1
Interview to Offer	Number of interviews held for each offer made	2 to 1
Time to Offer	Number of days between approved requirement in FG to offer made	12 working days
Time from Offer to On-board	Time from offer extended to a completed on-board (issue of verification record) made for all roles closed within the previous month	10 working days
C-SAT - Hiring Manager Satisfaction	% of responses Satisfied or above	85%
C-SAT - Candidate Satisfaction	% of responses Satisfied or above	85%
Rate Alignment	% candidates at or below the rate set out on the rate cart	85%
Aged Requirements	% of roles closed within 30 days from approved requirement in FG to offer made	90%
Fieldglass Availability	% of time the VMS is available for service (working hours)	99.99%

Admin and Clerical KPI targets

KPIs				
Measure		Target	Min. acceptable level	Measurement period
KPI 1	**Time to Offer**	Average of 8 working days	Average of 10 working days	Monthly
KPI 2	**Time to Onboard**	Average of 8 working days	Average of 10 working days	Monthly
KPI 3	**Client Satisfaction**	85%	80%	Monthly
KPI 4	**Candidate Satisfaction**	85%	80%	Monthly
KPI 5	**Rate Alignment**	100%	100%	Quarterly

[redacted]

Appendix 6

Standard Contract Clauses

Appendix 6 Controller
to Controller Standard

Appendix 6: Controller to Controller Standard Contractual Clauses

[Note : To be populated in collaboration Parties respective Data Protection Officers]

CONTROLLER TO CONTROLLER STANDARD CONTRACTUAL CLAUSES

Data transfer agreement

between

Alexander Mann Solutions Limited
7 Bishopsgate
London
EC2N 3AQ
United Kingdom

hereinafter "**data exporter**")

and

..... (name)

..... (address and country of establishment) [TO BE COMPLETED]

hereinafter "**data importer**"

each a "**party**"; together "**the parties**".

Definitions

For the purposes of the clauses:

"**personal data**", "**special categories of data/sensitive data**", "**process/processing**", "**controller**", "**processor**", "**data subject**", and "**supervisory authority/authority**" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby the "**authority**" shall mean the competent data protection authority in the territory in which the data exporter is established);

"**clauses**" shall mean these contractual clauses which are a free standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements;

"**data exporter**" shall mean the controller who transfers the personal data; and

"**data importer**" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

1. Obligations of the data exporter

The data exporter warrants and undertakes that:

1.1 the personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter;

1.2 it has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses;

1.3 it will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established;

1.4 it will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time; and

1.5 it will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause 3, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

2. Obligations of the data importer

The data importer warrants and undertakes that:

2.1 it will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected;

2.2 it will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data;

2.3 it has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws;

2.4 it will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses;

2.5 it will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed the data importer will assume responsibility for compliance with the provisions of clause 1.5;

2.6 at the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause 3 (which may include insurance coverage);

2.7 upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion;

2.8 it will process the personal data, at its option, in accordance with:

2.8.1 the data protection laws of the country in which the data exporter is established; or

2.8.2 the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data imported complies with the relevant provisions of such an authorisation or decision and is based in a country to which such authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data; or

2.8.3 the data processing principles set forth in Annex A:

2.8.3.1 Data importer to indicate which option it selects: 2.8.3

2.8.3.2 Initials of data importer deemed included

2.9 It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer; and

2.9.1 the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection; or

2.9.2 the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU; or

2.9.3 data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards; or

2.9.4 with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer.

3. Liability and third party rights

3.1 Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (ie damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

3.2 The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses 1.2, 1.4, 1.5, 2.1, 2.3, 2.4, 2.5, 2.9, 3.1, 5, 6.3 and 7 against the data importer or the data exporter, for their respective breach of their contractual obligations with regard to his personal data and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by that data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer, if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

4. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause 2.8 which shall apply only if so selected by the data importer under that clause.

5. Resolution of disputes with data subjects or the authority

5.1 In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

5.2 The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

5.3 Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

6. Termination

6.1 In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

6.2 In the event that:

6.2.1 the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph 6.1;

6.2.2 compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligation in the country of import;

6.2.3 The data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

6.2.4 a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter;

6.2.5 a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs;

6.2.6 then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by 6.2.1, 6.2.2 or 6.2.5 above the data importer may also terminate these clauses.

6.3 Either party may terminate these clauses if:

6.3.1 any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer; or

6.3.2 Directive (95/46/EC (or any superseding text) becomes directly applicable in such country.

6.4 The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause 6.2) does not exempt them

from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

7. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

8. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause 1.5. The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

ANNEX A: DATA PROCESSING PRINCIPLES

1. **Purpose limitation:** Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. **Data quality and proportionality**: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. **Transparency:** Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. **Security and confidentiality:** Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. **Rights of access, rectification, deletion and objection:** As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. **Sensitive data:** The data importer shall take such additional measures (eg relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause 2.

7. **Data used for marketing purposes:** Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt out" from having his data used for such purposes.

8. **Automated decisions:** For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects

concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

8.1 (i) such decisions are made by the data importer in entering into or performing a contract with the data subject; and

(ii) the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties; or

8.2 where otherwise provided by the law of the data exporter.

[redacted]

ANNEX B: DESCRIPTION OF THE TRANSFER

[*To be completed by the parties*]
Data subjects
The personal data transferred concern the following categories of data subjects: [*Contingent labour staff supplied by Alexander Mann Solutions Limited*]

Purpose of the transfer(s)
The transfer is made for the following purposes: [*Alexander Mann Solutions Limited to transfer contingent labour personal data to the Data Importer, when requested. The purpose of the transfer is to allow the Data Importer to undertake audits of the Alexander Mann Solutions Limited onboarding process of contingent labour staff.*]

Categories of data
The personal data transferred concern the following categories of data: [*Name, email address, postal address, national insurance number, telephone number, date of birth, place of birth, gender, nationality, immigration status, employment history, criminal convictions and offences and passport number*]

Recipients
The personal data transferred may be disclosed only to the following recipients or categories of recipients: [*To be used internally within the Data Importer for audit purposes only.*]

Sensitive data (if appropriate)
The personal data transferred concern the following categories of sensitive data: [*Criminal convictions and offences.*]

Data processing registration information of the data exporter (*ICO Registration Number Z6924746)*

Additional useful information (N/A)

Contact points for data protection enquiries

DATA EXPORTER

[redacted]

DATA IMPORTER

Name:
Position:
Email:

[redacted]

Appendix 7

NHS Digital Security Policy

Appendix 7 NHSD
Personal Security & V

[redacted]

NHS Digital

Personnel Security and Vetting Policy			
Status		Approved	
Document Record ID Key			
Version	<V1.0>	Version Date	27/04/2018
Director Responsible for this policy	[redacted]		
Person to contact about this policy	[redacted]		
Author	[redacted]		

Personnel Security and Vetting Policy

Contents

1. Policy Statement

The policy **shall** be used to ensure the appropriate level of personnel security controls are applied consistently throughout NHS Digital.

2. Purpose

The purpose of the policy is to adopt HMG guidelines[1] to safeguard NHS Digital assets and IT systems and to provide a level of assurance as to the trustworthiness, integrity and reliability of all staff.

3. Scope

The policy relates to all staff that have access to NHS Digital assets, IT systems, buildings, information and other UK Government information.

4. Equality Impact Assessment

An equality impact assessment (EIA) has been completed and can be viewed at Annex A.

5. Terminology

Term	Definition
SHALL	This term is used to state a **Mandatory** requirement of this policy
SHOULD	This term is used to state a **Recommended** requirement of this policy
MAY	This term is used to state an **Optional** requirement

6. Applicability

The policy **shall** apply to all NHS Digital staff and temporary employees (e.g. consultants, contractors, work package resources, resource company employees).

7. Levels of Personnel Security Controls

7.1. Baseline Personnel Security Standard (BPSS)

All staff **shall** hold a minimum level of BPSS for the duration of their employment.

7.2. National Security Vetting

Staff who have been identified as requiring National Security Vetting (CTC, SC or DV) clearance **shall** undertake the process in accordance with NHS Digital guidance.

[1] HMG Personnel Security Controls V3.0 December 2017 Final

8. Legal/Risk Mitigation

NHS Digital **shall** take into the consideration the below legislation in respect of undertaking BPSS and National Security Vetting.

- Data Protection Act 1998 and subsequent DPA 2018
- General Data Protection Regulation
- Fraud Act 2006

9. Roles and Responsibilities

9.1. Human Resources

HR **shall** ensure that all pre-employment checks are carried out in accordance with NHS Digital guidance.

9.2. Third Party Suppliers

Third party suppliers **shall** supply evidence that they hold the correct level of personnel security controls for the work they are required to undertake. If this cannot be produced a risk assessment and appropriate sign off **shall** be undertaken by the responsible person procuring their services.

9.3. ICT

ICT **shall** ensure that access to systems is not granted prior to confirmation of BPSS compliance from HR.

9.4. Managers

In accordance with NHS Digital guidance managers **shall** ensure that staff have attained the appropriate level of personnel security controls before granting access to NHS Digital systems and designated secure areas. In the unlikely event that staff commence employment without the relevant personnel security controls in place the manager **shall** ensure that a risk assessment has been completed as per NHS Digital guidance.

9.5. Office Services

Office Services **shall** ensure that access to buildings is not granted prior to confirmation of BPSS from HR. If access to designated secure areas is required Office Services **shall** seek approval from the relevant manager prior to granting access.

9.6. Staff

Staff **shall** inform the organisation of any change of personal circumstances in accordance with NHS Digital guidance. Staff **shall** undertake any further process when instructed by the Vetting Officer in accordance with NHS Digital guidance. During the course of employment staff **shall** disclose immediately to their manager if they are charged or convicted of any criminal offence; this may, dependent upon the nature of the conviction, result in disciplinary action being taken up to and including dismissal.

9.7. Vetting Officer

The Vetting Officer **shall** ensure that all policy and guidance is under frequent review in line with Department of Health and Social Care, HMG and UKSV policy. The Vetting Officer **shall** inform the member of staff when their vetting renewal is due.

9.8. SIRO

The Senior Information Risk Owner retains overall accountability for the policy.

10. Unsatisfactory BPSS or Vetting Checks

All unsatisfactory BPSS or national security vetting checks **shall** be dealt with in accordance with Personnel Security and Vetting Policy Guidance and any other relevant NHS Digital guidance.

11. Appeals Process (National Security Vetting)

All appeals and enquiries related to national security vetting **shall** be dealt with in accordance with Personnel Security and Vetting Policy Guidance and any other relevant NHS Digital guidance.

12. Incident Reporting

Any breach of this policy is an information security incident and **shall** be reported in accordance with the Information Security Incident Policy.

Annexe A – Equality Impact Assessment

Business area	Live Services Directorate
Team/Unit	Data Security Centre
Date	09/04/2018

Name of Policy/Guidance/Operational activity
Personnel Security and Vetting Policy and Guidance

What are the aims, objectives & projected outcomes?
The policy shall be used to ensure the appropriate level of personnel security controls are applied consistently to all staff throughout NHS Digital. The purpose of the policy is to adopt HMG guidelines to safeguard NHS Digital assets and IT systems and to provide a level of assurance as to the trustworthiness, integrity and reliability of all staff. The policy relates to all staff that have access to NHS Digital assets, IT systems, buildings, information and other UK Government information. The projected outcome is that all staff within NHS Digital have the correct level of personnel security controls, minimum of which is a Baseline Personnel Security Standard (BPSS) over the next 18 months to 24 months before the move into the Leeds Government Hub Building.

This is a **new** policy/guidance/operational activity.	**Yes**
This is a **change** to an existing policy/guidance/operational activity (Check original policy was equality impact assessed. If so, review and update action plan).	**No**
This is an **existing** policy/guidance/operational activity.	**No**
Will the policy/guidance have an impact on national or local people/staff?	**Yes**
Are particular communities or groups likely to have different needs, experiences and/or attitudes in relation to the policy/guidance?	**No**
Are there any aspects of the policy/guidance that could contribute to equality or inequality?	**No**
Could the aims of the policy/guidance be in conflict with equal opportunity, elimination of discrimination or fostering good relations?	**No**

If your answer to any of these questions is **YES**, go on to the full EIA. **Or** Where you are satisfied due regard has already been met through the policy development process give details of the findings/outcomes and provide the evidence below. If you have answered **NO** to all of these questions then please provide appropriate evidence and sign off.	

This policy/guidance was screened for impact on equalities. The following evidence has been considered.
NHS Digital have a responsibility to ensure we do everything within our power to build public trust. As such we should meet government standards for the application of minimum recruitment controls, as outlined in the Security Policy Framework and HMG Personnel Security Controls. These standards describe the pre-employment screening controls for employees within government and are applicable to non-departmental public bodies, who support the critical national infrastructure. At the basic level this requires our organisation to ensure **all** employees meet the Baseline Personnel Security Standard (BPSS), which includes the verification of: • Identity • Employment history (past three years) • Nationality and immigration (right to work) status • Criminal records check (unspent convictions only) NHS Digital already collects Identity, Employment History and Nationality and Immigration and has introduced the criminal records check within our recruitment process for new starters (from 1 February 2018) and now needs to roll out to the current workforce. To meet these minimum standards all current employees will be required to undertake a Basic Disclosure check, to return evidence of any unspent convictions, as defined by the Rehabilitation of Offenders Act 1974. All staff are affected equally by this policy – for any staff who require a higher level of security check than BPSS further guidance has been produced. Staff will need to complete an on-line form, scan a copy of their identification documents (usually passport and driver's licence) and send to staffvetting.com (our partner company who will facilitate the checks). The documents will be validated by HR/workforce staff and the results sent to the individual and recruitment team. Process are in place to assist staff with this

requirement by providing guidance, named individuals, a dedicated mailbox and Frequently Asked Questions document – available in all formats available to NHS Digital staff. Only the staff members themselves and the recruitment/workforce manager will see the outcome of the disclosure and this will be held by the individual. In the case of a positive disclosure there is a process where individuals will be seen on a case by case basis, by a 'Disclosure Panel' which includes members from HR Business Partners and Data Security Centre. This approach has been developed cross-organisationally including colleagues from HR, Data Security Centre (DSC), Business Delivery and Communications. All agree that all staff will be affected equally by this policy and there is no discrimination in terms of; Race, Religion, Disability, Sex, Gender Reassignment, Sexual Orientation, Age and Human Rights.

SCS or senior manager sign-off	[redacted]
I have read the preliminary screening and I am satisfied that given the available evidence, a full Equality Impact Assessment is not required. ***OR*** ***I have read the available evidence and I am satisfied that due regard (in line with the Quality Assurance criteria and/or the full EIA template) has been demonstrated and that that this evidence has/will be published.***	
Date	
Review Date (where applicable)	

Document Management

Revision History

Version	Date	Summary of Changes
0.1	05/04/18	Initial draft for comment
0.2	11/04/18	Comments incorporated from [redacted], [redacted] and [redacted]
0.3	17/04/18	Comments incorporated from [redacted] and [redacted]

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
[redacted]		05/04/18	0.1
		11/04/18	0.2
		11/04/18	0.2
		10/04/18	0.1
		09/04/18	0.1

Approved by

This document must be approved by the following people:

Name	Signature	Title	Date	Version
[redacted]			20/04/2018	0.3
			13/04/2018	0.2
COG Board			26/04/2018	0.3

NB. The version of the policy posted on the intranet must be a pdf copy of the signed approved version.

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of the document are not controlled.

[redacted]

Appendix 8

NHS Digital ICT Policy

[redacted]

Appendix 10

Business Continuity and Disaster Recovery

[redacted]

Appendix 12

Customer's IR35 Process

Appendix 12 IR35
Process Guidance Note

Process Guidance Notes:

Definitions:

NHSD	NHS Digital
CEST	HMRC Check Employment Status for Tax tool
Contractor	the Worker
SMART	Specific, Measurable, Achievable, Reasonable and Time Bound
IR35 Function	The NHS Digital Function responsible for making IR35 assessments [redacted]
FCAP	The NHS Digital Finance and Commercial Assurance Panel
IR35 Assessor	NHS Digital's nominated independent IR35 Assessor (currently QDOS)
PSBC	Professional Services Business Case
PSBC Review	Review of the PSBC by the responsible HR, Finance and Commercial functions

Background:

In April 2000, IR35 was introduced by Gordon Brown in order to clamp down on what he saw as 'disguised employment'. Between then and April 2017, the onus was on the contractor to show that he was compliant with the legislation. After April 2017, the onus was transferred from contractors working in the public sector to the End Client making NHSD responsible for the correct treatment of IR35.

This document describes the actions being taken by NHSD to manage IR35 and the resultant process for implementing these actions. Note that, whilst Contingent Suppliers will be requested to support it, this is an NHSD process.

Actions NHS Digital (NHSD) are taking:

In addition to requesting that any proposed worker completes the rudimentary CEST tool provided by HMRC, NHSD is taking further steps to ensure that our risk exposure for contractors working outside IR35 is reduced further. For the avoidance of doubt, if either:

- the CEST tool; or
- NHSD's assessment; or
- independent in-situ assessment

concludes the role is in-side scope or in any way in doubt then the worker shall be treated as in-scope.

A summary of actions being taken includes:

1. For Outside-IR35 Contractors, gaining assurance that substitution is acceptable by:
    a. Obtaining sign off by the Exec Director in charge of the project that they are prepared to accept this.
    b. Assuring ourselves that the assignment title reflects the actual assignment and not be a 'generic role'.
    We do understand that for recruitment and statistical purposes we still use generic job descriptions but we need to reflect the specific assignment that the contractor is being asked to deliver.
    c. Gaining prior commitment from the contractor that they will provide a substitute and helpers if required. (This will also reduce confusion about their right of substitution and how it works etc.)

2. Financial Risk
    a. Contractors who are outside scope of IR35 will cease to be paid on the basis of the time they work. Instead they will be paid for achieving milestones. This will have some further impacts:
        i. The milestones will be as outlined in the Assessment form complete with initial agreed dates and values.
        ii. Once each milestone has been reached the contractor will be paid the amount shown on the assessment regardless of when completed. Should the milestone be significantly delayed a provision of a part payment may be considered.
        iii. In cases where SMART (Specific, Measurable, Achievable, Reasonable and Time Bound) milestones are not initially available that there is a refinement process in place to ensure they become SMART prior to starting delivery (Agile).

3. Independent IR35 Assessments
    a. Contractors who are outside the scope of IR35 are required to obtain an independent initial IR35 in-situ assessment within 30 days of starting the assignment. In the event that such an assessment deems the situation to be in scope, NHS Digital – at their discretion - may either:
        i. Correct operation of the relationship to ensure truly outside of scope; or
        ii. Take the necessary steps to bring the relationship inside the scope of IR35
    b. Such independent in-situ assessments shall be refreshed at 6 monthly intervals as a means of ensuring continued adherence to outside IR35 requirements
    c. In the very unlikely event that Admin and Clerical (or Temporary Workers) are agreed to be outside the scope of IR35, NHS Digital will handle the cost as an agreed expense to be submitted by the Contractor
    d. For Specialists operating outside the scope of IR35, NHS Digital deem the cost of such assessments to be part of the service provided by the Specialist (and the Specialist shall carry the cost of these assessments)

4. Contracts must be time bound. Once a contractor finishes a contract they cannot, unless specifically agreed by the IR35 Function, be offered a new outside IR35 contract for six months (especially within the similar area of activity)

5. Ex-employees cannot be engaged as being out of scope contractors until after a year has passed. Such workers must not be coming back to resume the role that they were doing as an employee.

6. All out of scope contractors are required to evidence their 'badges of business'.
   For information, this is in the form of a questionnaire (Appendix 2). Each question is weighted and contributes to determining if a business is truly in existence. For example a contractor who has been in business for several years, has other directors/employees, has an office separate to their own home, has a website/stationery and provides specialist equipment etc. receives a much higher score that someone whose company was established immediately prior to commencing their contract with NHSD, has no other clients / directors

The Process for bringing on Contractors

At a high level the process for Contractors involves:

1. Determining if the Contractor is falls into the scope of PSBC cover and ensuring it is in place
2. Determining if the Assignment falls inside or outside of IR35
3. Determining if the Contractors situation is such that they fall inside IR35
4. If outside IR35 continuously managing the Contractor on the basis of agreed milestones (not time and materials) and
5. If outside, routinely obtaining assurance that IR35 compliance is maintained

Putting in place PSBC cover where needed

It is strongly recommended that the business area / programme put in place an overarching PSBC as part of their annual business planning process or as a part of any programme business cases.

However, should there be no covering PSBC, regardless of whether inside or outside the scope of IR35:

1. Determine if PSBC cover is required (applicable to all Contractors who are paid a day rate equivalent to an NHS Agenda For Change Band 8a and above. If required the following steps must be followed:

2. Create necessary PSBC paperwork to include:
    a. The scope of the project
    b. Whether the requirement is for a 'Specialist Contractor' (outside scope) or an 'Interim Manager' (Inside scope) or a combination of both.
    c. If the requirement is for a 'Specialist Contractor' the PSBC needs to show the following:
        i. What the specialism is
        ii. Why this specialism is not something that NHSD has available at the time

    If the requirement is for 'Interim Managers' (i) and (ii) are not required.

3. Once the PSBC has been completed it needs to submitted for PSBC Review and following this FCAP who will endorse (or not) prior to submitting it for formal approval.
    Note that, depending on the value and/or nature of the PSBC, different levels of approval will be necessary (and such approvals may take time).

Determination of the Applicability of IR35

4. For the sake of clarity, if the Worker is acting as an interim in any way they are inside the scope of IR35.

The following process only applies if a 'Specialist Contractor' deemed to be potentially outside the scope of IR35:

5. To appoint a specialist contractor, a 'Contractor Assessment Form' is required (see appendix 1).
    a. If not a 'nominated worker' this form will be required to be processed twice
        i. firstly in draft (without the name of the contractor, their PSC and how milestones will be delivered) and
        ii. then as a final version including the details below
    b. If the specialist contractor is a 'nominated worker' the form should immediately include the name of the contractor, their PSC and a proposal on how the milestones will be delivered. This will only be processed once.

6. This form (as an initial draft if the Contractor not known, and final version when known will require to go to the IR35 Function for review and comment. Assuming approved, this form should then be:
    a. Wet or electronically signed by the Hiring Manager;
    b. Signed or separately endorsed by email by the Directorate Lead (to confirm acceptance of substitutes, etc.);
    c. Submitted to FCAP for 'noting' (capturing evidence that the process has been followed).

Assessing the Contractor

7. Once the individual is known, in addition to ensuring that there is a fully completed Contractor Assessment Form, the individual will also be required to complete a separate NHSD IR35 Risk Assessment Form (Appendix 2). This provides assurance (over and above the basic CEST test) that the individuals situation with respect to their organisation and history with NHSD does not introduce IR35 related risks.

8. This Form must also be sent to the IR35 Function for review and comment.
Regardless of the status assessed via the Contractor Assessment Form, if the risk identified via this process is deemed anything other than Low, the combination of individual and role will be also be deemed to be within the scope of IR35.

9. Both forms (the IR35 Risk Assessment and Contractor Assessment) should form part of the final submission to FCAP for 'noting'.

Continuously Managing an Outside-IR35 Contractor

Assuming endorsed, the outside-IR35 contractor, once security checks and other onboarding activities have been completed, is able to start work. However, the IR35 risk extends beyond the initial assignment phase. There is an ongoing responsibility on the Hiring Manager and the Contractor to ensure that the work remains outside IR35.

10. In order for the Contractor to receive full payment for the period, they and their Hiring Manager are required to sign off the agreed milestones in accordance with the agreed acceptance criteria. The contractor will not be paid for that milestone until the milestone is completed. Any required rectification needed to fully deliver the milestone (unless clearly evidenced and agreed as outside the control of the contractor) must be rectified at the contractors cost. Completed Milestone certificates (which may cover more than one milestone) should be signed off by the Hiring Manager and sent to the IR35 Function.

11. Typically at the same time, the Contractor and Hiring Manager shall agree refinements to any future Milestones. Once committed to (which must be in advance of starting delivery of any specific Milestone), the Milestone becomes fixed. Provided there is no material change in the overarching scope of work Future Milestones may be deleted, new replacement Milestones added and, up to the point of commitment, existing Milestones refined (Agile working). The Hiring Manager and Contractor are jointly responsible for maintaining a full audit path to evidence any such refinement.

Assurance that Outside IR35 Requirements are being met

12. Within 30 days of starting an assignment, the Contractor is required to have undertaken an independent in-situ (versus documentation based) IR35 assessment by the IR35 Assessor. If assessed as being in-scope, and unless corrective actions are taken to manage compliantly – confirmed by the assessor - the assignment will move in-scope.
    The certificate and results arising from this assessment should be sent to the IR35 Function.

13. The Contractor is responsible for refreshing the independent in-situ IR35 assessment described under (9) on each 6 month anniversary of the assignment. Certificates should continue to be sent to the IR35 Function.

Appendix 1

NHS Digital Assignment Specification

[Title of Assignment]

([Specifics if applicable])

[High level goal of the assignment. This should link to a project or programme to emphasise the fact that this is a finite piece of work. A change in this goal will represent a material change to the Assignment terms (requiring a new Assignment Specification).

Background and the high level goal of the assignment.

Term of the Assignment

Specific Work Objectives

PSBC No.					
Milestone No	Description	Milestone Value	Anticipated End date	Actual End date	Milestone Sign off

Other Obligations

Section 2 – milestone details

Contractor:	**[Organisation (versus named individual)]**
Contact:	**[Accountable contact within the organisation]**
Assignment:	[Per the Assignment Specification]
Period:	[The dates to and from covered by this reporting] [the complete report should be no more than 1-2 pages]

Previously Agreed Deliverable Status:			
No	Output	Status[1]	Issues Arising
	[Description of the required deliverable]		

Breakdown of tasks:			
No	Breakdown of tasks to achieve the deliverable	Type[2]	How Delivered
	[Description of rectification or additional output]		

[1] Status: **Done**, In Progress, Rectified, On Hold, Deleted: If not Done or within the control of the individual the Cause should explain why
[2] Type: New, Fixed: How Delivered should highlight if delivered outside normal working hours.

Outputs for Next Period:			
No	Output	Priority[3]	Comment
	[Brief description of the outputs required in the next period]	[see note]	[Any clarifications]

Risks, Issues & Opportunities:			
No	Description	H/M/L	Recommendation (Mitigation)
	[Highlight anything which should be monitored]		

Other Comments:
[Whatever is useful]

Signed by:	[On behalf of the contractor]	Date:	

Agreed by:	[The name of the accountable manager]	Date:	

[3] Priority: MoSCoW. (M)ust Do, (S)hould Do, (C)ould Do (and (W)ont Do – not used). All Musts must be done, Shoulds should be.

For a role to be considered for an out of scope of IR35 assessment, the accountable individual must agree to all the below statements. If these cannot be agreed to in full, the role will be assessed as inside scope.

Right of Substitution
NHS Digital contracts with a Personal Service Company (PSC) via an Intermediary (normally the recruitment agency). The PSC provides the contractor. If the contractor is unable to complete all or part of the contract, the PSC may supply a substitute or helper. NHS Digital may not nominate a substitute In order for the right of substitution to exist, the PSC must engage, train and pay for the substitute. The PSC is fully responsible for the work carried out by the substitute and should the work be unsatisfactory or not completed within an agreed timescale, NHS Digital reserves the right to withhold or reduce any agreed payments during the term of the substitution until the work has been brought up to an acceptable standard. In light of the above, NHS Digital can only refuse a substitute where they are not suitably skilled, qualified, security cleared or not able to perform the original contractor's duties. However, NHS Digital cannot undertake any form of interview or other assessment and must accept the PSC's confirmation of the substitute's ability for the role.
Right of Control
The Contractor is responsible for the What, Where, How and When the contract is carried out. To fulfil this criteria, the focus must be specifically on the outputs that the contractor must fulfil, with minimal input from the hiring manager. In addition, there must be no restrictions on where the contractor is located and also no restrictions on the hours that they are expected to work, provided the targets outlined in section 2 are met by the expected date.
Financial Risk
HMRC expects a PSC to have a financial risk for the work undertaken. The more the financial risk there is, the greater the chance of the contractor working for the PSC being outside of scope of IR35. When the schedule of tasks has been agreed between the parties, it is the responsibility of the contractor to fulfil the tasks within the timeframe allocated. With certain exceptions (i.e. unforeseen delays that are outside the control of the contractor), the contractor must complete the tasks within that time frame and cost. If the contractor fails to deliver a task or the task delivered is not to an acceptable standard, the contractor is required to complete or 'make good' the work in their own time and expense.
Reporting and Audit Records
NHS Digital and the contractor are both accountable for ensuring compliance with IR35 is auditable. To this end the reports (illustrated in section 2) should be stored and be able to be retrieved on request.
PSBC Reference / Other Comments:
[Reference to PSBC Cover]

Accountable Individual:	[The name of the individual who will approve the outputs]	Position:	[Position of the individual]
Signed	[Signature of the above individual]	Date:	
Approved by:	[The name of the executive director]		
Signed by:	[The name of the above director]	Date:	

Appendix 2 – NHS Digital IR35 Risk Assessment Form.

Contractor Questionnaire

Contractor Name _____

Name of Company _____

Company Registation Number _____

1	Has the current end client engaged you on PAYE employment terms within the 12 months which ended on the last 31st March with no major changes to your working arrangements If you are doing the same work, the answer to the question is Yes Note: Working at a different location does not count as a major change	Please Choose: No
2	How long have you been engaged with NHS Digital?	Please Choose: More than 2 years
3	Does your business own or rent business premises which are separate both from your home and from the end client's premises?	Please Choose: Yes
4	How long has your business been in operation?	Please Choose: More than 2 years
5	Does your business engage any workers who bring in at least 25% of your yearly turnover? If your intermediary is a company these workers need to be people other than directors or shareholders of the company If your intermediary is a parnership these workers need to be people other than parners in the partnership	Please Choose: Yes
6	Has your company undertaken any separtate contracts concurrent with this engagement?	Please Choose: Yes
7	Do you have your own stationery / website?	Please Choose: Yes
8	Does your company own any assets such as Equipment, Bank account etc.	Please Choose: Yes
9	Could you provide a named indiviual that you could call upon as a substitute if required?	Please Choose: Yes

10 Have you ever excercised a right to provide a substitute for this particular contract?	Please Choose: No
If yes, could you provide the name of the substitute, the dates of the substitution and the cirumstances that arose to necessicate the substitution.	
11 Have you ever engaged helpers that are not part of NHS Digital to assist in providing a significant amount of the services, for this particular contract?	Please Choose: No
If yes, could you provide details	
12 Have you paid for equipment or training, which is vital to the provision of your services through your company?	Please Choose: Yes
If so, please give details	
13 What expenses do you claim from NHS Digital in relation to travel and/or accomodation?	Please Choose: and expenses out of my own pocket.
Note: This includes travel claimed through expenses as well as travel booked through NHS Digital's booking system.	
14 Do you have Professional Indemnity Insurance & Employers Liability Insurance?	Please Choose: Yes
15 Has your Hiring Manager agreed target/milestones/deliverables for you to achieve?	Please Choose: Yes
16 Are you paid upon the delivery of milestones or on a daily/hourly rate?	Please Choose: Hourly / daily rate
17 Have you had to rectfy faulty work or had to work additional hours to reach a milestone at your own time and expense - if so please give details	Please Choose: No
18 Did you record this on your ABR Timesheet	Please Choose: No
Status	Low Risk

[redacted]

Signature Area