Order Form

1. Contract Reference	DFERPPU/ 22-23/085
2. Date	15th August 2023
3. Buyer	The Department for Education 2 Sanctuary Buildings, Great Smith Street, London, SW1P 3BT
4. Supplier	**UNIVERSITY OF DURHAM,** whose legal address is The Palatine Centre, Stockton Road, Durham, DH1 3LE, United Kingdom.
5. The Contract	The Supplier shall supply the deliverables described below on the terms set out in this Order Form and the attached contract conditions ("**Conditions**") and any *Annexes*. Unless the context otherwise requires, capitalised expressions used in this Order Form have the same meanings as in Conditions. In the event of any conflict between this Order Form and the Conditions, this Order Form shall prevail. Please do not attach any Supplier terms and conditions to this Order Form as they will not be accepted by the Buyer and may delay conclusion of the Contract.
6. Services	The evaluation will use quasi-experimental methods (a pre/post study and regression discontinuity analysis) to assess whether Pupil Premium funding has reduced between-school segregation and/or reduced the attainment gap. The analysis will use the PPMD and NPD data sets. Key Deliverables: • Project inception: Initial steering group meeting, receive data files, start initial analysis (scope out data and possibilities). • Main analysis: initial findings (shared with DfE) internal presentation of methods to share learning within DfE Draft report of findings. • Final publishable report of findings. • Monthly update meetings To be performed at Durham University (School of Education Durham University Leazes Road Durham DH1 1TA) or home-working set up

7. Specification	The specification of the Deliverables is as set out in Annex 2.
8. Term	The Term shall commence on 2nd October 2023 and the expiry date shall be 4th November 2024, unless it is otherwise extended or terminated in accordance with the terms and conditions of the Contract. The Buyer may extend the Contract for a period of up to 6 months by giving not less than 10 Working Days' notice in writing to the Supplier prior to the Expiry Date. The terms and conditions of the Contract shall apply throughout any such extended period.
9. Charges	**£75,000** excluding VAT The Charges for the Deliverables shall be as set out in Annex 3.
10. Payment	All invoices must be sent, quoting a valid purchase order number (PO Number), to: Accountspayable.ocr@education.gov.uk Within **10** Working Days of receipt of your countersigned copy of this letter, we will send you a unique PO Number. You must be in receipt of a valid PO Number before submitting an invoice. To avoid delay in payment it is important that the invoice is compliant and that it includes a valid PO Number, PO Number item number (if applicable) and the details (name and telephone number) of your Buyer contact (i.e. Contract Manager). Non-compliant invoices will be sent back to you, which may lead to a delay in payment. If you have a query regarding an outstanding payment, please contact our Accounts Payable section either by email to Accountspayable.ocr@education.gov.uk or ***card.finance@education.gov.uk***
11. Buyer Authorised Representative (s)	For general liaison your contact will continue to be Chief Research Officer – [redacted] [redacted] And [redacted] [redacted] .

12. Address for notices	**Buyer: The Department for Education** The Department for Education Sanctuary Buildings, Great Smith Street, London, SW1P 3BT Attention: [redacted] **Supplier: Durham University.** Attention: For the attention of Legal Services, Durham University, The Palatine Centre, Stockton Road, Durham, DH1 3LE, United Kingdom.
14. Procedures and Policies	The Buyer may require the Supplier to ensure that any person employed in the delivery of the Deliverables has undertaken a Disclosure and Barring Service check. The Supplier shall ensure that no person who discloses that he/she has a conviction that is relevant to the nature of the Contract, relevant to the work of the Buyer, or is of a type otherwise advised by the Buyer (each such conviction a "**Relevant Conviction**"), or is found by the Supplier to have a Relevant Conviction (whether as a result of a police check, a Disclosure and Barring Service check or otherwise) is employed or engaged in the provision of any part of the Deliverables.

Signed for and on behalf of the **Supplier**	Signed for and on behalf of the **Buyer**
Name:	Name:
Date: 11/08/23	Date: 14/08/23
Signature:	Signature:

Annex 1 – Authorised Processing Template

Contract:	**Pupil Premium Evaluation -** 22-23/085
Date:	15th August 2023
Description Of Authorised Processing	The processing is needed in order to evaluate the impact of the Pupil Premium. The two data-sets (PPMD and NPD) will enable the contractor to measure the change in segregation and the attainment gap, for pupils before and after the introduction of Pupil Premium.
Subject matter of the processing	Attainment, demographic and financial data from the National Pupil Database (NPD) and Parent, Pupil matched dataset (PPMD).
Duration of the processing	12-month contract (approximately 6 months of processing)
Nature and purposes of the processing	Data analysis to evaluate the impact of government policy and inform future spending
Type of Personal Data	Attainment data, income data and FSM status are the main variables used. No identifying data will be used (Pupil matching reference will be used to pseudonymise the data)
Categories of Data Subject	De-identified personal level data: Category B data – children in care. Category C data – free school meal eligibility. Category D data – ethnicity and SEN. Category E data – attainment data.

Annex 2 – Specification

Background

Pupil Premium policy was implemented in England in 2011 and provides additional funding to schools (c£2.5bn p.a.) to accelerate the progress and boost the attainment of disadvantaged pupils of all abilities in England. Because the policy was applied to all schools and areas it was not possible to design an evaluation with a clear counterfactual group which did not receive Pupil Premium funding.

Subsequent research has been limited by being too early, weak and/or small scale. More recently, Durham academics have conducted before-and-after time series analyses which attempts to control for the impact of other confounding factors, including changes to the law, the economy and to pupil assessment, that have taken place over the same period (Stephen Gorard, 2022). However, their work is limited by having no access to pupil-level household income and benefits data.

The department has now obtained a dataset that combines pupil-level National Pupil Database (NPD)/Census data with HMRC (income) and DWP (benefits) data – the parent pupil matched data set (PPMD) This provides an opportunity to improve on previous work.

Aims

To understand the impact of Pupil Premium funding on between-school segregation and the disadvantage attainment gap.

Method

The DfE will provide the contractor with the NPD and PPMD data sets. The contractor will use PPMD data to identify whether outcomes for otherwise similar pupils and schools vary subject to differences in their exposure to Pupil Premium treatment, with the overall aim of identifying whether the Pupil Premium can causally account for differences in attainment outcomes and school intake. The contractor will use quasi-experimental approaches in line with the established education literature, for example regression discontinuity design, difference in differences, or regression analysis. We anticipate that the analysis will be exploratory, and the contractor will have freedom to conduct further analysis where deemed appropriate (ie with specific groups of pupils). The contractor will provide interim findings to the Department and a draft report (that allows for at least two rounds of edits). The final report should contain sufficient detail on methods of analysis used, so that the analysis can be replicated by others with access to the data. The report should be in a standard that is publishable.

Milestones/deliverables		Date
Project inception - Receive data files - Start initial analysis (scope out data and possibilities)	The contractor will access the data sets via the ONS SRS. The processing will occur at Durham university in a secure area (SRS) in their office suite. The contractor will also attend regular steering groups organised by DfE, to provide insight and overview of the ongoing project (minimum three meetings).	October 2023

	Once familiar with the data set, the codes/methods used should be shared with DfE and ETF.	
Contractor communication	Contractor shall provide comprehensive updates and regular communication (at least monthly) on progress, risks, issues and forthcoming activities. Either through meetings with the project lead or through steering group meetings.	Ongoing
Main analysis	The contractor will conduct two main types of analysis (regression discontinuity design analysis and pre/post analysis). Extra exploratory analysis should be considered where appropriate.	April 2024
Initial findings	Summary of main findings of the analysis should be presented.	June 2024
Additional exploratory analysis	Additional analysis may be required following initial findings	July 2024
Internal presentation of methods to share learning within DfE	Initial results and methodology should be shared with DfE. An interim presentation will be produced. These findings will be shared internally within the department prior to the finalised products.	July 2024
Draft report of findings.	The contractor will produce a research report that outlines the methodology and key findings of the analysis. The report will contain graphics and charts to aid dissemination of the data, with written narrative. The contractor will be expected to provide a draft to the department allowing for at least two rounds of comments.	September 2024
Final published report of findings.	Reporting should be completed using the Department for Education research report template and in line with the Department's style and formatting guide for research publications. The report should be provided in an accessible format so that it can be published on gov.uk.	October 2024

Annex 3 – Charges

Project Milestone	Payment Amount	Payment Date
Project Inception	[redacted]	31st October 2023
Data cleaning, scope out data and possibilities. Data Analysis Initial Findings	[redacted]	21st June 2024
Additional exploratory analysis based on feedback from initial findings Internal presentation of methods to share learning within DfE	[redacted]	23rd August 2024
At least two draft reports (to allow for two rounds of comments) Final Publishable report of findings	[redacted]	31st October 2024

Expenditure for the financial year 2023-2024 shall not exceed [redacted] of VAT.
Expenditure for the financial year 2024-2025 shall not exceed [redacted] of VAT.

Total Project expenditure shall not exceed £75,000 exclusive of VAT.

Annex 4 – Data

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

The contact details of the Controller's Data Protection Officer are: [redacted]
The contact details of the Processor's Data Protection Officer are: [redacted]
The processor shall comply with any further written instructions with respect to processing by the Controller.

Any such further instructions shall be incorporated into this Schedule.

Description	*Details*
Identity of the Controller and Processor	*The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor in accordance with Clause 7.1.*
Subject matter of the processing	*The processing is needed in order to evaluate the impact of the Pupil Premium. The two data-sets (PPMD and NPD) will enable the contractor to measure the change in segregation and the attainment gap, for pupils before and after the introduction of Pupil Premium.*
Duration of the processing	*October 2023– September 2024*
Nature and purposes of the processing	*The Processor will:* *Receive, by secure means, personal data from the PPMD and NPD, for the purpose of carrying out secondary analysis for the Pupil Premium Evaluation.* *These are data sets held by the DfE and will be made available via the ONS SRS.* *Store these personal data securely for the duration of the project.* *Only use the data sets for the permitted purposes of this project.* *Destroy any data files once processing is complete.*
Type of Personal Data being processed	*Personal data includes from the PPMD: child age, employment earnings, universal credit, adult income, adults in household, household income, children in household. From the NPD: school demographics (eg establishment type), attainment scores, anonymous pupil matching reference number, year group, academic year, free school meal status.*

	Special category data includes: children in care, ethnicity and SEN status. To note: these variables are optional and may be dropped if there are data sharing concerns. *All personal data will be non-identifiable due to the two data sets being linked by pupil matching reference (PMR's). No living individual will be capable of being identified from the information shared between the Parties. If, at a later date, it is necessary to share Personal Data as part of the arrangements contemplated by this Agreement then the Parties shall enter into a separate Data Sharing Agreement or Data Processing Agreement (as appropriate).*
Categories of Data Subject	*Pupils*
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	*The data will be retained for the duration of the contract, the sample files will be destroyed once there is no further justification to retain.* *The data will be made available via the ONS SRS. Once the licence period ends, ONS will remove the researcher's access to the data via their ONS SRS account and remove permission for them to enter the data labs before destroying the data according to the Memorandum of Understanding between DfE and ONS.*

Short form Terms

1. Definitions used in the Contract

In this Contract, unless the context otherwise requires, the following words shall have the following meanings:

"Central Government Body"	means a body listed in one of the following subcategories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: a) Government Department; b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c) Non-Ministerial Department; or d) Executive Agency;
"Charges"	means the charges for the Deliverables as specified in the Order Form;
"Confidential Information"	means all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (i) is known by the receiving Party to be confidential; (ii) is marked as or stated to be confidential; or (iii) ought reasonably to be considered by the receiving Party to be confidential;
"Contract"	means the contract between (i) the Buyer and (ii) the Supplier which is created by the Supplier's counter signing the Order Form and includes the Order Form and Annexes;
"Controller"	has the meaning given to it in the GDPR;
"Buyer"	means the person identified in the letterhead of the Order Form;
"Date of Delivery"	means that date by which the Deliverables must be delivered to the Buyer, as specified in the Order Form;
"Buyer Cause"	any breach of the obligations of the Buyer or any other default, act, omission, negligence or statement of the Buyer, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Buyer is liable to the Supplier;
"Data Protection Legislation"	(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the Data Protection Act 2018 to the extent that it relates to processing

	of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy;
"Data Protection Impact Assessment"	an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;
"Data Protection Officer"	has the meaning given to it in the GDPR;
"Data Subject"	has the meaning given to it in the GDPR;
"Data Loss Event"	any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;
"Data Subject Access Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
"Deliver"	means hand over the Deliverables to the Buyer at the address and on the date specified in the Order Form, which shall include unloading and any other specific arrangements agreed in accordance with Annex 2 Delivered and Delivery shall be construed accordingly;
"Existing IPR"	any and all intellectual property rights that are owned by or licensed to either Party and which have been developed independently of the Contract (whether prior to the date of the Contract or otherwise);
"Expiry Date"	means the date for expiry of the Contract as set out in the Order Form;
"FOIA"	means the Freedom of Information Act 2000 together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;
"Force Majeure Event"	any event, occurrence, circumstance, matter or cause affecting the performance by either Party of its obligations under the Contract arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control which prevent or materially delay it from performing its obligations under the Contract but excluding: i) any industrial dispute relating to the Supplier, the Supplier Staff (including any subsets of them) or any other failure in the Supplier or the Subcontractor's supply chain; ii) any event, occurrence, circumstance, matter or cause which is attributable to the wilful act, neglect or failure to take reasonable precautions against it by the Party concerned; and iii) any failure of delay caused by a lack of funds;
"GDPR"	the General Data Protection Regulation (Regulation (EU) 2016/679);

"Goods"	means the goods to be supplied by the Supplier to the Buyer under the Contract;
"Good Industry Practice"	standards, practices, methods and procedures conforming to the law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector;
"Government Data"	a) the 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, including any of the Buyer's confidential information, and which: i) are supplied to the Supplier by or on behalf of the Buyer; or ii) the Supplier is required to generate, process, store or transmit pursuant to the Contract; or b) any Personal Data for which the Buyer is the Data Controller;
"Information"	has the meaning given under section 84 of the FOIA;
"Information Commissioner"	the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;
"Insolvency Event"	in respect of a person: a) if that person is insolvent; ii) if an order is made or a resolution is passed for the winding up of the person (other than voluntarily for the purpose of solvent amalgamation or reconstruction); iii) if an administrator or administrative receiver is appointed in respect of the whole or any part of the persons assets or business; iv) if the person makes any composition with its creditors or takes or suffers any similar or analogous action to any of the actions detailed in this definition as a result of debt in any jurisdiction;
"Key Personnel"	means any persons specified as such in the Order Form or otherwise notified as such by the Buyer to the Supplier in writing;
"LED"	Law Enforcement Directive (Directive (EU) 2016/680);
"New IPR"	all and intellectual property rights in any materials created or developed by or on behalf of the Supplier pursuant to the Contract but shall not include the Supplier's Existing IPR;
"Order Form"	means the letter from the Buyer to the Supplier printed above these terms and conditions;
"Party"	the Supplier or the Buyer (as appropriate) and "Parties" shall mean both of them;
"Personal Data"	has the meaning given to it in the GDPR;
"Personal Data Breach"	has the meaning given to it in the GDPR;

"Processor"	has the meaning given to it in the GDPR;
"Purchase Order Number"	means the Buyer's unique number relating to the order for Deliverables to be supplied by the Supplier to the Buyer in accordance with the terms of the Contract;
"Regulations"	the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires) as amended from time to time;
"Request for Information"	has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term "request" shall apply);
"Services"	means the services to be supplied by the Supplier to the Buyer under the Contract;
"Specification"	means the specification for the Deliverables to be supplied by the Supplier to the Buyer (including as to quantity, description and quality) as specified in the Order Form;
"Staff"	means all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any sub-contractor of the Supplier engaged in the performance of the Supplier's obligations under the Contract;
"Staff Vetting Procedures"	means vetting procedures that accord with good industry practice or, where applicable, the Buyer's procedures for the vetting of personnel as provided to the Supplier from time to time;
"Subprocessor"	any third Party appointed to process Personal Data on behalf of the Supplier related to the Contract;
"Supplier Staff"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under a Contract;
"Supplier"	means the person named as Supplier in the Order Form;
"Term"	means the period from the start date of the Contract set out in the Order Form to the Expiry Date as such period may be extended in accordance with clause [11.2] or terminated in accordance with the terms and conditions of the Contract;
"US-EU Privacy Shield Register"	a list of companies maintained by the United States of America Department for Commence that have self-certified their commitment to adhere to the European legislation relating to the processing of personal data to non-EU countries which is available online at: https://www.privacyshield.gov/list;

"VAT"	means value added tax in accordance with the provisions of the Value Added Tax Act 1994;
"Workers"	any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurementpolicynote-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables;
"Working Day"	means a day (other than a Saturday or Sunday) on which banks are open for business in the City of London.

2. Understanding the Contract

In the Contract, unless the context otherwise requires:

2.1 references to numbered clauses are references to the relevant clause in these terms and conditions;

2.2 any obligation on any Party not to do or omit to do anything shall include an obligation not to allow that thing to be done or omitted to be done;

2.3 the headings in this Contract are for information only and do not affect the interpretation of the Contract;

2.4 references to "writing" include printing, display on a screen and electronic transmission and other modes of representing or reproducing words in a visible form;

2.5 the singular includes the plural and vice versa;

2.6 a reference to any law includes a reference to that law as amended, extended, consolidated or re-enacted from time to time and to any legislation or byelaw made under that law; and

2.7 the word ‘including’, "for example" and similar words shall be understood as if they were immediately followed by the words "without limitation".

3. How the Contract works

3.1 The Order Form is an offer by the Buyer to purchase the Deliverables subject to and in accordance with the terms and conditions of the Contract.

3.2 The Supplier is deemed to accept the offer in the Order Form when the Buyer receives a copy of the Order Form signed by the Supplier.

3.3 The Supplier warrants and represents that its tender and all statements made and documents submitted as part of the procurement of Deliverables are and remain true and accurate.

4. What needs to be delivered

4.1 All Deliverables

(a) The Supplier must provide Deliverables: (i) in accordance with the Specification; (ii) to a professional standard; (iii) using reasonable skill and care; (iv) using Good Industry Practice; (v) using its own policies, processes and internal quality control measures as long as they don't conflict with the Contract; (vi) on the dates agreed; and (vii) that comply with all law.

4.2

5. Pricing and payments

5.1 In exchange for the Deliverables, the Supplier shall be entitled to invoice the Buyer for the charges in the Order Form. The Supplier shall raise invoices promptly and in any event within 90 days from when the charges are due.

5.2 All Charges:

(a) exclude VAT, which is payable on provision of a valid VAT invoice;

(b) include all costs connected with the supply of Deliverables.

5.3 The Buyer must pay the Supplier the charges within 30 days of receipt by the Buyer of a valid, undisputed invoice, in cleared funds to the Supplier's account stated in the Order Form.

5.4 A Supplier invoice is only valid if it:

(a) includes all appropriate references including the Purchase Order Number and other details reasonably requested by the Buyer;

(b) includes a detailed breakdown of Deliverables which have been delivered (if any).

5.5 If there is a dispute between the Parties as to the amount invoiced, the Buyer shall pay the undisputed amount. The Supplier shall not suspend the provision of the Deliverables unless the Supplier is entitled to terminate the Contract for a failure to pay undisputed sums in accordance with clause 11.6. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause 33.

5.6 The Buyer may retain or set-off payment of any amount owed to it by the Supplier if notice and reasons are provided.

5.7 The Supplier must ensure that all subcontractors are paid, in full, within 30 days of receipt of a valid, undisputed invoice. If this doesn't happen, the Buyer can publish the details of the late payment or non-payment.

6. The Buyer's obligations to the Supplier

6.1 If Supplier fails to comply with the Contract as a result of a Buyer Cause:

(a) the Buyer cannot terminate the Contract under clause 11;

(b) the Supplier is entitled to reasonable and proven additional expenses and to relief from liability under this Contract;

(c) the Supplier is entitled to additional time needed to deliver the Deliverables; (d) the Supplier cannot suspend the ongoing supply of Deliverables.

6.2 Clause 6.1 only applies if the Supplier:
(a) gives notice to the Buyer within 10 Working Days of becoming aware;
(b) demonstrates that the failure only happened because of the Buyer Cause; (c) mitigated the impact of the Buyer Cause.

7. Record keeping and reporting

7.1 The Supplier must ensure that suitably qualified representatives attend progress meetings with the Buyer and provide progress reports when specified in the Order Form.

7.2 The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Contract for seven years after the date of expiry or termination of the Contract.

7.3 The Supplier must allow any auditor appointed by the Buyer access to their premises to verify all contract accounts and records of everything to do with the Contract and provide copies for the audit.

7.4 The Supplier must provide information to the auditor and reasonable co-operation at their request.

7.5 If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:
(a) tell the Buyer and give reasons;
(b) propose corrective action;
(c) provide a deadline for completing the corrective action.

7.6 If the Buyer, acting reasonably, is concerned as to the financial stability of the Supplier such that it may impact on the continued performance of the Contract then the Buyer may:
(a) require that the Supplier provide to the Buyer (for its approval) a plan setting out how the Supplier will ensure continued performance of the Contract and the Supplier will make changes to such plan as reasonably required by the Buyer and once it is agreed then the Supplier shall act in accordance with such plan and report to the Buyer on demand
(b) if the Supplier fails to provide a plan or fails to agree any changes which are requested by the Buyer or fails to implement or provide updates on progress with the plan, terminate the Contract immediately for material breach (or on such date as the Buyer notifies).

8. Supplier staff

8.1 The Supplier Staff involved in the performance of the Contract must:
(a) be appropriately trained and qualified;
(b) be vetted using Good Industry Practice and in accordance with Staff Vetting procedures;
(c) comply with all conduct requirements when on the Buyer's premises.

8.2 Where a Buyer decides one of the Supplier's Staff isn’t suitable to work on the Contract, the Supplier must replace them with a suitably qualified alternative.

8.3 If requested, the Supplier must replace any person whose acts or omissions have caused the Supplier to breach clause 8.

8.4 The Supplier must provide a list of Supplier Staff needing to access the Buyer's premises and say why access is required.

8.5 The Supplier indemnifies the Buyer against all claims brought by any person employed by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.

8.6 The Supplier shall use those persons nominated in the Order Form (if any) to provide the Deliverables and shall not remove or replace any of them unless:
(a) requested to do so by the Buyer (not to be unreasonably withheld or delayed);
(b) the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or
(c) the person's employment or contractual arrangement with the Supplier or any subcontractor is terminated for material breach of contract by the employee.

9. Rights and protection

9.1 The Supplier warrants and represents that:
(a) it has full capacity and authority to enter into and to perform the Contract;
(b) the Contract is executed by its authorised representative;
(c) it is a legally valid and existing organisation incorporated in the place it was formed;
(d) there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its affiliates that might affect its ability to perform the Contract;
(e) it maintains all necessary rights, authorisations, licences and consents to perform its obligations under the Contract;
(f) it doesn't have any contractual obligations which are likely to have a material adverse effect on its ability to perform the Contract; and (g) it is not impacted by an Insolvency Event.

9.2 The warranties and representations in clause 9.1 are repeated each time the Supplier provides Deliverables under the Contract.

9.3 The Supplier indemnifies the Buyer against each of the following:
(a) wilful misconduct of the Supplier, any of its subcontractor and/or Supplier Staff where such wilful misconduct impacts the Contract;
(b) non-payment by the Supplier of any tax or National Insurance.

9.4 If the Supplier becomes aware of a representation or warranty that becomes untrue or misleading, it must immediately notify the Buyer.

9.5 All third party warranties and indemnities covering the Deliverables must be assigned for the Buyer's benefit by the Supplier.

10. Intellectual Property Rights (IPRs)

10.1 Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable worldwide licence to use, change and sub-license the Supplier's Existing IPR to enable it and its sublicensees to both:

(a) receive and use the Deliverables;
(b) use the New IPR.

10.2 Any New IPR created under the Contract is owned by the Buyer. The Buyer gives the Supplier a licence to use any Existing IPRs for the purpose of fulfilling its obligations under the Contract and a perpetual, royalty-free, non-exclusive licence to use any New IPRs.

10.3 Where a Party acquires ownership of intellectual property rights incorrectly under this Contract it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.

10.4 Neither Party has the right to use the other Party's intellectual property rights, including any use of the other Party's names, logos or trademarks, except as provided in clause 10 or otherwise agreed in writing.

10.5 If any claim is made against the Buyer for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Deliverables (an "**IPR Claim**"), then the Supplier indemnifies the Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result of the IPR Claim.

10.6 If an IPR Claim is made or anticipated the Supplier must at its own expense and the Buyer's sole option, either:
(a) obtain for the Buyer the rights in clauses 10.1 and 10.2 without infringing any third party intellectual property rights;
(b) replace or modify the relevant item with substitutes that don't infringe intellectual property rights without adversely affecting the functionality or performance of the Deliverables.

11. Ending the contract

11.1 The Contract takes effect on the date of or (if different) the date specified in the Order Form and ends on the earlier of the date of expiry or termination of the Contract or earlier if required by Law.

11.2 The Buyer can extend the Contract where set out in the Order Form in accordance with the terms in the Order Form.

11.3 Ending the Contract without a reason

The Buyer has the right to terminate the Contract at any time without reason or liability by giving the Supplier not less than 90 days' written notice and if it's terminated clause 11.5(b) to 11.5(g) applies.

11.4 When the Buyer can end the Contract

(a) If any of the following events happen, the Buyer has the right to immediately terminate its Contract by issuing a termination notice in writing to the Supplier:
(i) there's a Supplier Insolvency Event;
(ii) if the Supplier repeatedly breaches the Contract in a way to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms and conditions of the Contract;
(iii) if the Supplier is in material breach of any obligation which is capable of remedy, and that breach is not remedied within 30 days of the Supplier

receiving notice specifying the breach and requiring it to be remedied;

(iv) there's a change of control (within the meaning of section 450 of the Corporation Tax Act 2010) of the Supplier which isn't pre-approved by the Buyer in writing;

(v) if the Buyer discovers that the Supplier was in one of the situations in 57 (1) or 57(2) of the Regulations at the time the Contract was awarded;

(vi) the Court of Justice of the European Union uses Article 258 of the Treaty on the Functioning of the European Union (TFEU) to declare that the Contract should not have been awarded to the Supplier because of a serious breach of the TFEU or the Regulations;

(vii) the Supplier or its affiliates embarrass or bring the Buyer into disrepute or diminish the public trust in them.

(b) If any of the events in 73(1) (a) to (c) of the Regulations (substantial modification, exclusion of the Supplier, procurement infringement) happen, the Buyer has the right to immediately terminate the Contract and clause 11.5(b) to 11.5(g) applies.

11.5 What happens if the Contract ends

Where the Buyer terminates the Contract under clause 11.4(a) all of the following apply:

(a) the Supplier is responsible for the Buyer's reasonable costs of procuring replacement deliverables for the rest of the term of the Contract;

(b) the Buyer's payment obligations under the terminated Contract stop immediately;

(c) accumulated rights of the Parties are not affected;

(d) the Supplier must promptly delete or return the Government Data except where required to retain copies by law;

(e) the Supplier must promptly return any of the Buyer's property provided under the Contract;

(f) the Supplier must, at no cost to the Buyer, give all reasonable assistance to the Buyer and any incoming supplier and co-operate fully in the handover and re-procurement;

(g) the following clauses survive the termination of the Contract: [3.2.10, 6, 7.2, 9, 11, 14, 15, 16, 17, 18, 34, 35] and any clauses which are expressly or by implication intended to continue.

11.6 When the Supplier can end the Contract

(a) The Supplier can issue a reminder notice if the Buyer does not pay an undisputed invoice on time. The Supplier can terminate the Contract if the Buyer fails to pay an undisputed invoiced sum due and worth over 10% of the total Contract value or £1,000, whichever is the lower, within 30 days of the date of the reminder notice.

(b) If a Supplier terminates the Contract under clause 11.6(a):

(i) the Buyer must promptly pay all outstanding charges incurred to the Supplier;

(ii) the Buyer must pay the Supplier reasonable committed and unavoidable losses as long as the Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Contract had not been terminated;

(iii) clauses 11.5(d) to 11.5(g) apply.

11.7 Partially ending and suspending the Contract

(a) Where the Buyer has the right to terminate the Contract it can terminate or suspend (for any period), all or part of it. If the Buyer suspends the Contract it can provide the Deliverables itself or buy them from a third party.

(b) The Buyer can only partially terminate or suspend the Contract if the remaining parts of it can still be used to effectively deliver the intended purpose.

(c) The Parties must agree (in accordance with clause 24) any necessary variation required by clause 11.7, but the Supplier may not either:

(i) reject the variation;

(ii) increase the Charges, except where the right to partial termination is under clause 11.3.

(d) The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under clause 11.7.

12. How much you can be held responsible for

12.1 Each Party's total aggregate liability under or in connection with the Contract (whether in tort, contract or otherwise) is no more than 125% of the Charges paid or payable to the Supplier.

12.2 No Party is liable to the other for:

(a) any indirect losses;

(b) loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect).

12.3 In spite of clause 12.1, neither Party limits or excludes any of the following:

(a) its liability for death or personal injury caused by its negligence, or that of its employees, agents or subcontractors;

(b) its liability for bribery or fraud or fraudulent misrepresentation by it or its employees;

(c) any liability that cannot be excluded or limited by law.

12.4 In spite of clause 12.1, the Supplier does not limit or exclude its liability for any indemnity given under clauses, 8.5, 9.3, 13.2or 14.26(e).
If any third party makes a claim, or notifies an intention to make a claim, against the Buyer which may reasonably be considered likely to give rise to a liability under this clause (“Claim”), the Buyer shall:

i. as soon as reasonably practicable, give written notice of the Claim to the Supplier specifying the nature of the Claim in reasonable detail;

ii. not make any admission of liability, agreement or compromise in relation to the Claim without the prior written consent of the Supplier, provided that the Buyer may settle the Claim (after giving prior written notice of the terms of settlement (to the extent legally possible) to the Supplier, but without obtaining the Supplier's consent) if the Buyer reasonably believes that failure to settle the Claim would be prejudicial to it in any material respect.

iii. give the Supplier and its professional advisers access at reasonable times (on reasonable prior notice) to its premises and its officers, directors, employees, agents, representatives or advisers, and to any relevant assets, accounts, documents and records within the power or control of the Buyer them and where able to take copies (at the Supplier's expense) for the purpose of assessing the Claim; and

iv. take such action as the Supplier may reasonably request to avoid, dispute, compromise or defend the Claim.

12.5 Each Party must use all reasonable endeavours to mitigate any loss or damage which it suffers under or in connection with the Contract, including any indemnities.

12.6 If more than one Supplier is party to the Contract, each Supplier Party is fully responsible for both their own liabilities and the liabilities of the other Suppliers.

13. Obeying the law

13.1 The Supplier must, in connection with provision of the Deliverables, use reasonable endeavours to:

(a) comply and procure that its subcontractors comply with the Supplier Code of Conduct appearing at (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779660/20190220-Supplier_Code_of_Conduct.pdf) and such other corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time;

(b) support the Buyer in fulfilling its Public Sector Equality duty under S149 of the Equality Act 2010;

(c) not use nor allow its subcontractors to use modern slavery, child labour or inhumane treatment;

(d) meet the applicable Government Buying Standards applicable to Deliverables which can be found online at: https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs

13.2 The Supplier indemnifies the Buyer against any costs resulting from any default by the Supplier relating to any applicable law to do with the Contract.

13.3 The Supplier must appoint a Compliance Officer who must be responsible for ensuring that the Supplier complies with Law, Clause 13.1 and Clauses 27 to 32

13.4 "Compliance Officer" the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;

14. Data protection

14.1 The Buyer is the Controller and the Supplier is the Processor for the purposes of the Data Protection Legislation.

14.2 The Supplier must process Personal Data and ensure that Supplier Staff process Personal Data only in accordance with this Contract.

14.3 The Supplier must comply with the data procedures and clauses set out in the Data Sharing Agreement.

14.4 The Supplier must not remove any ownership or security notices in or relating to the Government Data.

14.5 The Supplier must make accessible back-ups of all Government Data, stored in an agreed off-site location and send the Buyer copies every six Months.

14.6 The Supplier must ensure that any Supplier system holding any Government Data, including back-up data, is a secure system that complies with the security requirements specified [in writing] by the Buyer.

14.7 If at any time the Supplier suspects or has reason to believe that the Government Data provided under the Contract is corrupted, lost or sufficiently degraded, then the Supplier must notify the Buyer and immediately suggest remedial action.

14.8 If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Buyer may either or both:
(a) tell the Supplier to restore or get restored Government Data as soon as practical but no later than five Working Days from the date that the Buyer receives notice, or the Supplier finds out about the issue, whichever is earlier; (b) restore the Government Data itself or using a third party.

14.9 The Supplier must pay each Party's reasonable costs of complying with clause 14.7 unless the Buyer is at fault.

14.10 Only the Buyer can decide what processing of Personal Data a Supplier can do under the Contract and must specify it for the Contract using the template in Annex 1 of the Order Form (*Authorised Processing*).

14.11 The Supplier must only process Personal Data if authorised to do so in the Annex to the Order Form (*Authorised Processing*) by the Buyer. Any further written instructions relating to the processing of Personal Data are incorporated into Annex 1 of the Order Form.

14.12 The Supplier must give all reasonable assistance to the Buyer in the preparation of any Data Protection Impact Assessment before starting any processing, including:
(a) a systematic description of the expected processing and its purpose;
(b) the necessity and proportionality of the processing operations;
(c) the risks to the rights and freedoms of Data Subjects;
(d) the intended measures to address the risks, including safeguards, security measures and mechanisms to protect Personal Data.

14.13 The Supplier must notify the Buyer immediately if it thinks the Buyer's instructions breach the Data Protection Legislation.

14.14 The Supplier must put in place appropriate Protective Measures to protect against a Data Loss Event which must be approved by the Buyer.

14.15 If lawful to notify the Buyer, the Supplier must notify it if the Supplier is required to process Personal Data by Law promptly and before processing it.

14.16 The Supplier must take all reasonable steps to ensure the reliability and integrity of any Supplier Staff who have access to the Personal Data and ensure that they: (a) are aware of and comply with the Supplier's duties under this clause 11;
(b) are subject to appropriate confidentiality undertakings with the Supplier or any Subprocessor;
(c) are informed of the confidential nature of the Personal Data and do not provide any of the Personal Data to any third Party unless directed in writing to do so by the Buyer or as otherwise allowed by the Contract;
(d) have undergone adequate training in the use, care, protection and handling of Personal Data.

14.17 The Supplier must not transfer Personal Data outside of the EU unless all of the following are true:

(a) it has obtained prior written consent of the Buyer;
(b) the Buyer has decided that there are appropriate safeguards (in accordance with Article 46 of the GDPR);
(c) the Data Subject has enforceable rights and effective legal remedies when transferred;
(d) the Supplier meets its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred;
(e) where the Supplier is not bound by Data Protection Legislation it must use its best endeavours to help the Buyer meet its own obligations under Data Protection Legislation; and
(f) the Supplier complies with the Buyer's reasonable prior instructions about the processing of the Personal Data.

14.18 The Supplier must notify the Buyer immediately if it:

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

14.19 Any requirement to notify under clause 14.17 includes the provision of further information to the Buyer in stages as details become available.

14.20 The Supplier must promptly provide the Buyer with full assistance in relation to any Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 14.17. This includes giving the Buyer:

(a) full details and copies of the complaint, communication or request;
(b) reasonably requested assistance so that it can comply with a Data Subject Access Request within the relevant timescales in the Data Protection Legislation;
(c) any Personal Data it holds in relation to a Data Subject on request;
(d) assistance that it requests following any Data Loss Event;
(e) assistance that it requests relating to a consultation with, or request from, the Information Commissioner's Office.

14.21 The Supplier must maintain full, accurate records and information to show it complies with this clause 14. This requirement does not apply where the Supplier employs fewer than 250 staff, unless either the Buyer determines that the processing:

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

14.22 The Supplier must appoint a Data Protection Officer responsible for observing its obligations in this Schedule and give the Buyer their contact details.

14.21 Before allowing any Subprocessor to process any Personal Data, the Supplier must:
(a) notify the Buyer in writing of the intended Subprocessor and processing;
(b) obtain the written consent of the Buyer;
(c) enter into a written contract with the Subprocessor so that this clause 14 applies to the Subprocessor;
(d) provide the Buyer with any information about the Subprocessor that the Buyer reasonably requires.

14.23 The Supplier remains fully liable for all acts or omissions of any Subprocessor.

14.24 At any time the Buyer can, with 30 Working Days notice to the Supplier, change this clause 14 to:
(a) replace it with any applicable standard clauses (between the controller and processor) or similar terms forming part of an applicable certification scheme under GDPR Article 42;
(b) ensure it complies with guidance issued by the Information Commissioner's Office.

14.25 The Parties agree to take account of any non-mandatory guidance issued by the Information Commissioner's Office.

14.26 The Supplier:
(a) must provide the Buyer with all Government Data in an agreed open format within 10 Working Days of a written request;
(b) must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading;
(c) must securely destroy all Storage Media that has held Government Data at the end of life of that media using Good Industry Practice;
(d) securely erase all Government Data and any copies it holds when asked to do so by the Buyer unless required by Law to retain it;
(e) indemnifies the Buyer against any and all Losses incurred if the Supplier breaches clause 14 and any Data Protection Legislation.

15. What you must keep confidential

15.1 Each Party must:
(a) keep all Confidential Information it receives confidential and secure;
(b) not disclose, use or exploit the disclosing Party's Confidential Information without the disclosing Party's prior written consent, except for the purposes anticipated under the Contract;
(c) immediately notify the disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information.

15.2 In spite of clause 15.1, a Party may disclose Confidential Information which it receives from the disclosing Party in any of the following instances:
(a) where disclosure is required by applicable Law or by a court with the relevant jurisdiction if the recipient Party notifies the disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure;
(b) if the recipient Party already had the information without obligation of confidentiality before it was disclosed by the disclosing Party;

(c) if the information was given to it by a third party without obligation of confidentiality;
(d) if the information was in the public domain at the time of the disclosure;
(e) if the information was independently developed without access to the disclosing Party's Confidential Information;
(f) to its auditors or for the purposes of regulatory requirements;
(g) on a confidential basis, to its professional advisers on a need-to-know basis;
(h) to the Serious Fraud Office where the recipient Party has reasonable grounds to believe that the disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010.

15.3 The Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Contract. The Supplier Staff must enter into a direct confidentiality agreement with the Buyer at its request.

15.4 The Buyer may disclose Confidential Information in any of the following cases: (a) on a confidential basis to the employees, agents, consultants and contractors of the Buyer;
(b) on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company that the Buyer transfers or proposes to transfer all or any part of its business to;
(c) if the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions;
(d) where requested by Parliament; (e) under clauses 5.7 and 16.

15.5 For the purposes of clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in clause 15.

15.6 Information which is exempt from disclosure by clause 16 is not Confidential Information.

15.7 The Supplier must not make any press announcement or publicise the Contract or any part of it in any way, without the prior written consent of the Buyer and must take all reasonable steps to ensure that Supplier Staff do not either.

16. When you can share information

16.1 The Supplier must tell the Buyer within 48 hours if it receives a Request For Information.

16.2 Within the required timescales the Supplier must give the Buyer full co-operation and information needed so the Buyer can:
(a) comply with any Freedom of Information Act (FOIA) request;
(b) comply with any Environmental Information Regulations (EIR) request.

16.3 The Buyer may talk to the Supplier to help it decide whether to publish information under clause 16. However, the extent, content and format of the disclosure is the Buyer's decision, which does not need to be reasonable.

16.4 Each party acknowledges that the other is subject to the requirements of the FOIA and the Environmental Information Regulations and shall assist and cooperate with the other to enable it to comply with its information disclosure obligations.

17. Invalid parts of the contract

If any part of the Contract is prohibited by Law or judged by a court to be unlawful, void or unenforceable, it must be read as if it was removed from that Contract as much as required and rendered ineffective as far as possible without affecting the rest of the Contract, whether it's valid or enforceable.

18. No other terms apply

The provisions incorporated into the Contract are the entire agreement between the Parties. The Contract replaces all previous statements and agreements whether written or oral. No other provisions apply.

19. Other people's rights in a contract

No third parties may use the Contracts (Rights of Third Parties) Act (CRTPA) to enforce any term of the Contract unless stated (referring to CRTPA) in the Contract. This does not affect third party rights and remedies that exist independently from CRTPA.

20. Circumstances beyond your control

20.1 Any Party affected by a Force Majeure Event is excused from performing its obligations under the Contract while the inability to perform continues, if it both:

(a) provides written notice to the other Party;

(b) uses all reasonable measures practical to reduce the impact of the Force Majeure Event.

20.2 Either party can partially or fully terminate the Contract if the provision of the Deliverables is materially affected by a Force Majeure Event which lasts for 90 days continuously.

20.3 Where a Party terminates under clause 20.2: (a) each party must cover its own losses; (b) clause 11.5(b) to 11.5(g) applies.

21. Relationships created by the contract

The Contract does not create a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

22. Giving up contract rights

A partial or full waiver or relaxation of the terms of the Contract is only valid if it is stated to be a waiver in writing to the other Party.

23. Transferring responsibilities

23.1 The Supplier cannot assign the Contract without the Buyer's written consent.

23.2 The Buyer can assign, novate or transfer its Contract or any part of it to any Crown Body, public or private sector body which performs the functions of the Buyer.

23.3 When the Buyer uses its rights under clause 23.2 the Supplier must enter into a novation agreement in the form that the Buyer specifies.

23.4 The Supplier can terminate the Contract novated under clause 23.2 to a private sector body that is experiencing an Insolvency Event.

23.5 The Supplier remains responsible for all acts and omissions of the Supplier Staff as if they were its own.

23.6 If the Buyer asks the Supplier for details about Subcontractors, the Supplier must provide details of Subcontractors at all levels of the supply chain including:
(a) their name;
(b) the scope of their appointment; (c) the duration of their appointment.

24. Changing the contract

24.1 Either Party can request a variation to the Contract which is only effective if agreed in writing and signed by both Parties. The Buyer is not required to accept a variation request made by the Supplier.

25. How to communicate about the contract

25.1 All notices under the Contract must be in writing and are considered effective on the Working Day of delivery as long as they're delivered before 5:00pm on a Working Day. Otherwise the notice is effective on the next Working Day. An email is effective when sent unless an error message is received.

25.2 Notices to the Buyer or Supplier must be sent to their address in the Order Form.

25.3 This clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

26. Preventing fraud, bribery and corruption

26.1 The Supplier shall not:
(a) commit any criminal offence referred to in the Regulations 57(1) and 57(2);
(b) offer, give, or agree to give anything, to any person (whether working for or engaged by the Buyer or any other public body) an inducement or reward for doing, refraining from doing, or for having done or refrained from doing, any act in relation to the obtaining or execution of the Contract or any other public function or for showing or refraining from showing favour or disfavour to any person in relation to the Contract or any other public function.

26.2 The Supplier shall take all reasonable steps (including creating, maintaining and enforcing adequate policies, procedures and records), in accordance with good industry practice, to prevent any matters referred to in clause 26.1 and any fraud by the Staff and the Supplier (including its shareholders, members and directors) in connection with the Contract and shall notify the Buyer immediately if it has reason to suspect that any such matters have occurred or is occurring or is likely to occur.

26.3 If the Supplier or the Staff engages in conduct prohibited by clause 26.1 or commits fraud in relation to the Contract or any other contract with the Crown (including the Buyer) the Buyer may:

(a) terminate the Contract and recover from the Supplier the amount of any loss suffered by the Buyer resulting from the termination, including the cost reasonably incurred by the Buyer of making other arrangements for the supply of the Deliverables and any additional expenditure incurred by the Buyer throughout the remainder of the Contract; or
(b) recover in full from the Supplier any other loss sustained by the Buyer in consequence of any breach of this clause.

27. Equality, diversity and human rights

27.1 The Supplier must follow all applicable equality law when they perform their obligations under the Contract, including:
(a) protections against discrimination on the grounds of race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise;
(b) any other requirements and instructions which the Buyer reasonably imposes related to equality Law.

27.2 The Supplier must take all necessary steps, and inform the Buyer of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on the Contract.

28. Tax

28.1 The Supplier must not breach any tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines. The Buyer cannot terminate the Contract where the Supplier has not paid a minor tax or social security contribution.

28.2 Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance contributions in the UK relating to payment received under the Off Contract, the Supplier must both:
(a) comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, the Social Security Contributions and Benefits Act 1992 (including IR35) and National Insurance contributions;
(b) indemnify the Buyer against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Contract Period in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff.

28.3 If any of the Supplier Staff are Workers who receive payment relating to the Deliverables, then the Supplier must ensure that its contract with the Worker contains the following requirements:
(a) the Buyer may, at any time during the term of the Contract, request that the Worker provides information which demonstrates they comply with clause 30.2, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding;
(b) the Worker's contract may be terminated at the Buyer's request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer;
(c) the Worker's contract may be terminated at the Buyer's request if the Worker provides information which the Buyer considers isn't good enough to

demonstrate how it complies with clause 30.2 or confirms that the Worker is not complying with those requirements;

(d) the Buyer may supply any information they receive from the Worker to HMRC for revenue collection and management.

29. Conflict of interest

29.1 The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual or potential conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to the Buyer under the Contract, in the reasonable opinion of the Buyer.

29.2 The Supplier must promptly notify and provide details to the Buyer if a conflict of interest happens or is expected to happen.

29.3 The Buyer can terminate its Contract immediately by giving notice in writing to the Supplier or take any steps it thinks are necessary where there is or may be an actual or potential conflict of interest.

30. Reporting a breach of the contract

30.1 As soon as it is aware of it the Supplier and Supplier Staff must report to the Buyer any actual or suspected breach of law, clause 13.1, or clauses 26 to 31.

30.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in clause 30.1.

31. Resolving disputes

31.1 If there is a dispute between the Parties, their senior representatives who have authority to settle the dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the dispute.

31.2 If the dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution (CEDR) Model Mediation Procedure current at the time of the dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the dispute, the dispute must be resolved using clauses 31.3 to 31.5.

31.3 Unless the Buyer refers the dispute to arbitration using clause 31.4, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:

(a) determine the dispute;
(b) grant interim remedies;
(c) grant any other provisional or protective relief.

31.4 The Supplier agrees that the Buyer has the exclusive right to refer any dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

31.5 The Buyer has the right to refer a dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under clause 31.3, unless the Buyer has agreed to the court proceedings or participated in them. Even if court

proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under clause 31.4.

31.4 The Supplier cannot suspend the performance of the Contract during any dispute.

32. Which law applies

This Contract and any issues arising out of, or connected to it, are governed by English law.

Special Terms

1. Safeguarding Children and Vulnerable Adults

"Regulated Activity"	In relation to children as defined in Part 1 of Schedule 4 to the Safeguarding Vulnerable Groups Act 2006. In relation to vulnerable adults as defined in Part 2 of Schedule 4 to the Safeguarding Vulnerable Groups Act 2006.

1.1 The Contractor will put in place safeguards to protect children and vulnerable adults from a risk of significant harm which could arise from the performance of this Contract. The Contractor will agree these safeguards with the Department before commencing work on the Contract.

1.2 In addition, the Contractor will carry out checks with the Disclosure and Barring Service (DBS checks) on all staff employed on the Contract in a Regulated Activity. Contractors must have a DBS check done every three years for each relevant member of staff for as long as this Contract applies. The DBS check must be completed before any of the Contractor's employees work with children in Regulated Activity.

1.3 The Contractor shall immediately notify the Department of any information that it reasona33bly requests to enable it to be satisfied that the obligations of this Clause [insert the clause number] have been met.

1.4 The Contractor shall not employ or use the services of any person who is barred from, or whose previous conduct or records indicate that he or she would not be suitable to carry out Regulated Activity or who may otherwise present a risk to children or vulnerable adults.

2. Project outputs

2.1 Unless otherwise agreed between the Contractor and the Project Manager, all outputs from the Project shall be published by the Department on the Department's research website.

2.2 The Contractor shall ensure that all outputs for publication by the Department adhere to the Department's Style Guide and MS Word Template, available to download from: Research reports: template and style guide - GOV.UK (www.gov.uk).

2.3 Unless otherwise agreed between the Contractor and Project Manager, the Contractor shall supply the Project Manager with a draft for comment at least eight weeks before the intended publication date, for interim reports, and eight weeks before the contracted end date, for final reports.

2.4 The Contractor shall consider revisions to the drafts with the Project Manager in the light of the Department's comments. The Contractor shall provide final, signed off interim reports and other outputs planned within the lifetime of the Project to the Department by no later than four weeks before the intended publication date, and final, signed off reports and other outputs at the end of the Project to the Department by no later than the contracted end date for the Project.

2.5 Until the date of publication, findings from all Project outputs shall be treated as confidential, as set out in the Clause 13 above. The Contractor shall not release findings to the press or disseminate them in any way or at any time prior to publication without approval of the Department.

2.6 Where the Contractor wishes to issue a Press Notice or other publicity material containing findings from the Project, notification of plans, including timing and drafts of planned releases shall be submitted by the Contractor to the Project Manager at least three weeks before the intended date of release and before any agreement is made with press or other external audiences, to allow the Department time to comment. All Press Notices released by the Department or the Contractor shall state the full title of the research report, and include a hyperlink to the Department's research web pages, and any other web pages as relevant, to access the publication/s. This clause applies at all times prior to publication of the final report.

2.7 Where the Contractor wishes to present findings from the Project in the public domain, for example at conferences, seminars, or in journal articles, the Contractor shall notify the Project Manager before any agreement is made with external audiences, to allow the Department time to consider the request. The Contractor shall only present findings that will already be in the public domain at the time of presentation, unless otherwise agreed with the Department. This clause applies at all times prior to publication of the final report.

3. Departmental Security Standards for Business Services and ICT Contracts

"BPSS" "Baseline Personnel Security Standard"	means the Government's HMG Baseline Personal Security Standard . Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard

"CCSC" "Certified Cyber Security Consultancy"	is the National Cyber Security Centre's (NCSC) approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. See website: https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy
"CCP" "Certified Professional"	is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession. See website: https://www.ncsc.gov.uk/information/about-certified-professional-scheme
"CPA" "Commercial Product Assurance" [formerly called "CESG Product Assurance"]	is an 'information assurance scheme' which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards.. See website: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa
"Cyber Essentials" "Cyber Essentials Plus"	Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme. There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to these providers: https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body
"Data" "Data Controller" "Data Protection Officer" "Data Processor" "Personal Data" "Personal Data requiring Sensitive Processing" "Data Subject", "Process" and "Processing"	shall have the meanings given to those terms by the Data Protection Act 2018
"Department's Data" "Department's Information"	is any data or information owned or retained in order to meet departmental business objectives and tasks, including: (a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible

	media, and which are: (i) supplied to the Contractor by or on behalf of the Department; or (ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or (b) any Personal Data for which the Department is the Data Controller;
"DfE" "Department"	means the Department for Education
"Departmental Security Standards"	means the Department's security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver.
"Digital Marketplace / G-Cloud"	means the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects.
End User Devices	means the personal computer or consumer devices that store or process information.
"Good Industry Practice" "Industry Good Practice"	means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
"Good Industry Standard" "Industry Good Standard"	means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
"GSC" "GSCP"	means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications
"HMG"	means Her Majesty's Government
"ICT"	means Information and Communications Technology (ICT) and is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution

“ISO/IEC 27001” “ISO 27001”	is the International Standard for Information Security Management Systems Requirements
“ISO/IEC 27002” “ISO 27002”	is the International Standard describing the Code of Practice for Information Security Controls.
“ISO 22301”	is the International Standard describing for Business Continuity
“IT Security Health Check (ITSHC)” “IT Health Check (ITHC)” “Penetration Testing”	means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.
“Need-to-Know”	means the Need-to-Know principle employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties.
“NCSC”	The National Cyber Security Centre (NCSC) is the UK government’s National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk
“OFFICIAL” “OFFICIAL-SENSITIVE”	the term ‘OFFICIAL’ is used to describe the baseline level of ‘security classification’ described within the Government Security Classification Policy (GSCP). the term ‘OFFICIAL–SENSITIVE is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the GSCP.
“RBAC” “Role Based Access Control”	means Role Based Access Control. A method of restricting a person’s or process’ access to information depending on the role or functions assigned to them.
“Storage Area Network” “SAN”	means an information storage system typically presenting block based storage (i.e. disks or virtual disks) over a network interface rather than using physically connected storage.
“Secure Sanitisation”	means the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. NCSC Guidance can be found at: https://www.ncsc.gov.uk/guidance/secur

	e-sanitisation-storage-media The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction
"Security and Information Risk Advisor" "CCP SIRA" "SIRA"	means the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also: https://www.ncsc.gov.uk/articles/about-certified-professional-scheme
"Senior Information Risk Owner" "SIRO"	means the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for overseeing the management of information risk across the organisation. This includes its executive agencies, arms length bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties.
"SPF" "HMG Security Policy Framework"	means the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government's Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. https://www.gov.uk/government/publications/security-policy-framework

3.1. The Contractor shall be aware of and comply the relevant HMG security policy framework, NCSC guidelines and where applicable DfE Departmental Security Standards for Contractors which include but are not constrained to the following clauses.

3.2. Where the Contractor will provide products or services or otherwise handle information at OFFICIAL for the Department, the requirements of Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - Action Note 09/14 dated 25 May 2016, or any subsequent updated document, are mandated, namely that contractors supplying products or services to HMG shall have achieved, and will be expected to retain Cyber Essentials certification at the appropriate level for the duration of the contract. The certification scope shall be relevant to the services supplied to, or on behalf of, the Department.

3.3. Where clause 3.2 above has not been met, the Contractor shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements).

The ISO/IEC 27001 certification must have a scope relevant to the services supplied to, or on behalf of, the Department. The scope of certification and the statement of applicability must be acceptable, following review, to the Department, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

3.4. The Contractor shall follow the UK Government Security Classification Policy (GSCP) in respect of any Departmental Data being handled in the course of providing this service and will handle all data in accordance with its security classification. (In the event where the Contractor has an existing Protective Marking Scheme then the Contractor may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Departmental Data).

3.5. Departmental Data being handled in the course of providing an ICT solution or service must be separated from all other data on the Contractor's or sub-contractor's own IT equipment to protect the Departmental Data and enable the data to be identified and securely deleted when required in line with clause 3.14.

3.6. The Contractor shall have in place and maintain physical security to premises and sensitive areas in line with ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access), CCTV, alarm systems, etc.

3.7. The Contractor shall have in place and maintain an appropriate user access control policy for all ICT systems to ensure only authorised personnel have access to Departmental Data. This policy should include appropriate segregation of duties and if applicable role based access controls (RBAC). User credentials that give access to Departmental Data or systems shall be considered to be sensitive data and must be protected accordingly.

3.8. The Contractor shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to:

- physical security controls;
- good industry standard policies and processes;
- malware protection;
- boundary access controls including firewalls, application gateways, etc;
- maintenance and use of fully supported software packages in accordance with vendor recommendations;
- use of secure device configuration and builds;
- software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;
- user identity and access controls, including the use of multi-factor authentication for sensitive data and privileged account accesses;
- any services provided to the department must capture audit logs for security events in an electronic format at the application, service and system level to meet the department's logging and auditing requirements, plus logs shall be:
    - retained and protected from tampering for a minimum period of six months;
    - made available to the department on request.

3.9. The contractor shall ensure that any departmental data (including email) transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.The contractor shall ensure that any departmental data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the department except where the department has given its prior written consent to an alternative arrangement.The contractor shall ensure that any device which is used to process departmental data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security and https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles.

3.10. Whilst in the Contractor's care all removable media and hardcopy paper documents containing Departmental Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.

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

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

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

3.12. In the event of termination of contract due to expiry, liquidation or non-performance, all information assets provided, created or resulting from the service shall not be considered as the supplier's assets and must be returned to the department and written assurance obtained from an appropriate officer of the supplying organisation that these assets regardless of location and format have been fully sanitised throughout the organisation in line with clause 3.15.

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

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

Evidence of secure destruction will be required in all cases.

3.14. Access by Contractor or sub-contractor staff to Departmental Data, including user credentials, shall be confined to those individuals who have a "need-to-know" in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Department. All Contractor or sub-contractor staff must complete this process before access to Departmental Data is permitted. Any Contractor or sub-contractor staff who will be in contact with children or vulnerable adults must, in addition to any security clearance, have successfully undergone an Enhanced DBS (Disclosure and Barring Service) check prior to any contact.

3.15. All Contractor or sub-contractor employees who handle Departmental Data shall have annual awareness training in protecting information.

3.16. The Contractor shall, as a minimum, have in place robust Business Continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the services delivered. If a ISO 22301 certificate is not available the supplier will provide evidence of the effectiveness of their ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures. This should include evidence that the Contractor has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.

3.17. Any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data, including user credentials, used or handled in the course of providing this service shall be recorded as an incident. This includes any non-compliance with these Departmental Security Standards for Contractors, or other Security Standards pertaining to the solution.

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

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

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

3.18. The Contractor shall ensure that any IT systems and hosting environments that are used to handle, store or process Departmental Data shall be

subject to independent IT Health Checks (ITHC) using an NCSC CHECK Scheme ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Department and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.

3.19. The Contractor or sub-contractors providing the service will provide the Department with full details of any actual or future intent to develop, manage, support, process or store Departmental Data outside of the EU mainland. The Contractor or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Department.

3.20. The Department reserves the right to audit the Contractor or sub-contractors providing the service within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being supplied and the Contractor's, and any sub-contractors', compliance with the clauses contained in this Section.

3.21. The Contractor and sub-contractors shall undergo appropriate security assurance activities and shall provide appropriate evidence including the production of the necessary security documentation as determined by the department. This will include obtaining any necessary professional security resources required to support the Contractor's and sub-contractor's security assurance activities such as: a Security and Information Risk Advisor (SIRA) certified to NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Cyber Professional (CCP) schemes.

3.22. Where the Contractor is delivering an ICT solution to the Department they shall design and deliver solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current NCSC Information Assurance Guidance and Departmental Policy. The Contractor will provide the Department with evidence of compliance for the solutions and services to be delivered. The Department's expectation is that the Contractor shall provide written evidence of:

- Compliance with HMG Minimum Cyber Security Standard.
- Any existing security assurance for the services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification.
- Any existing HMG security accreditations or assurance that are still valid including: details of the awarding body; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement.
- Documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Contractor shall provide details of who the awarding body or organisation will be and date expected.

3.23. The Contractor shall contractually enforce all these Departmental Security Standards for Contractors onto any third-party suppliers, sub-contractors or partners who could potentially access Departmental Data in the course of providing this service.