

ANNEX 1

LSE (IGC) SUPPLIER TERMS AND CONDITIONS (TERMS)

1. DEFINITIONS & INTERPRETATION

1.1 Definitions

In these Terms the following words and expressions have the following meanings:

"Annex"	means an annex attached to and forming part of the Contract;
"Appointment Letter"	means a letter of appointment issued by LSE to the Supplier in respect of the Services;
"Appropriate Authorities"	means relevant UK Authorities and/or government bodies or agencies in the territory where Serious Misconduct has or may have taken place which bodies or agencies have responsibility for safeguarding and/or investigating and/or taking legal action in respect of allegations of Serious Misconduct (which bodies or agencies may include local territory police forces and social services);
"Authorised Officer"	means a person authorised, either generally or specifically, by LSE in relation to the Contract;
"Background IPR"	means Intellectual Property Rights of a party developed prior to the Commencement Date or created independently of the Contract;
"Branding Guidelines"	means those brand guidelines for IGC and UK aid set out at: https://www.theigc.org/wp-content/uploads/2023/01/IGC-branding-one-pager.pdf
"Business Day"	means a day (other than a Saturday, Sunday or a public holiday) when banks in London are open for business;
"Charges"	means the charges payable by LSE for the supply of the Services constituting Fees which are either specified in the Appointment Letter or (if applicable) in Annex 2 and approved Expenses incurred in accordance with the Contract;
"Code of Conduct"	means the Supplier Code of Conduct set out in Annex 3 with which Suppliers must comply at the applicable level (and which also sets out their obligations in regard to monitoring of their performance in regard to such Code of Conduct) set out in Annex 3;
"Commencement Date"	means the date specified as the commencement date of the Contract in the Appointment Letter;
"Commercially Sensitive"	means information of a commercially sensitive nature relating to

Information"	the Supplier, its Intellectual Property Rights or its business or information which the Supplier has indicated to LSE that, if disclosed by LSE to a third party, would cause the Supplier significant commercial disadvantage or material financial loss;
"Compliance Level 2 Supplier"	means a supplier to LSE which is required to adhere to the Code of Conduct including in respect of the monitoring of its compliance with the Code of Conduct by virtue of the fact that the Supplier has an individual Contract value above the EU contracting threshold and below £1m, or two or more contracts with LSE, funded by FCDO, with a value of less than £5m.
"Confidential Information"	<p>means, in relation to a party to the Contract all confidential information of such party of any nature whatsoever including without limitation:</p> <p>(a) information concerning past, present and prospective finances, business dealings, systems, computer programmes, software, data, client and/or customer lists, contributors, suppliers, methods of doing business and information relating to any current or prospective business of such party;</p> <p>(b) (in relation to LSE as Disclosing Party) confidential information of FCDO and of other suppliers or of sub-contractors of LSE which is held by LSE;</p> <p>(c) any other information of a party obtained or received by the other party during the performance of the Services which is clearly confidential or ought reasonably to be considered confidential whether or not it is marked as "confidential";</p>
"Contract"	means the contract between LSE and the Supplier which agreement incorporates the Appointment Letter, these Terms and all other Annexes;
"Controller"	has the meaning given to it in Data Protection Law;
"Data Protection Law"	includes the Data Protection Act 2018 and the General Data Protection Regulation (EU) 2016/679); and all other applicable laws relating to the processing of personal data and privacy;
"Dispute"	means any dispute between the parties arising out of or in connection with the Contract or the performance, subsistence, validity or enforceability of any provisions of the Contract;
"Dispute Notice"	means a notice served by one party on the other in accordance with the provisions of Clause 18;
"Employment Taxes"	means income tax and/or national insurance contributions (including all payments to be made under the Income Tax (Earnings and Pensions) Act 2003, the Social Security Contributions and Benefits Act 1992) arising from or in connection with any payment or benefit received by any Supplier

	Personnel in respect of any Services completed or provided hereunder;
"Ethical Walls"	means a process for avoiding conflicts of interest by limiting disclosure of information to certain individuals within an organisation thereby building a metaphorical wall between the holders of information and colleagues who represent interests or hold opinions which conflict;
"Expenses"	means expenses properly incurred by the Supplier in the performance of obligations under the Contract and approved by LSE in accordance with the terms of the Contract;
"FCDO"	means HMG Secretary of State for Foreign, Commonwealth and Development Affairs at the Foreign, Commonwealth and Development Office (formerly Department for International Development) at Abercrombie House Hairmyres East Kilbride Glasgow G75 8EA;
"FCDO Contract"	means the contract between LSE and FCDO dated 27 September 2019 pursuant to which LSE is funded by FCDO to operate the International Growth Centre;
"FCDO Information"	means any FCDO information, data (including FCDO Personal Data), databases, reports and other materials (in any format or medium) which may be provided by LSE to the Supplier in connection with or pursuant to the Contract;
"FCDO Personnel"	means FCDO employees, consultants, suppliers, sub-contractors and agents;
"Fees"	means fees payable by LSE to the Supplier in consideration of the provision of the Services (including, where relevant, payments in respect of research awards);
"FOIA"	means the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and any subordinate legislation made under this Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government Department in relation to such legislation;
"Good Industry Practice"	means the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would be reasonably expected from a leading expert supplier of services similar to the Services where such supplier is seeking to comply with its contractual obligations in full and complying with applicable laws;
"HMG"	means His Majesty's Government of the United Kingdom;
"IGC"	means the International Growth Centre which is managed and

	operated by LSE;
"IGC Approved Project Information/Budget"	means (if applicable) the document at Annex 2 which, if applied for through the IGC's commissioning board is an abridged version of the final project proposal submitted by the Supplier or for non-commissioning board projects, is the finalised project proposal form, which sets out project design, aims and timelines for the provision of Services;
"Information"	means information held by the Supplier on behalf of LSE in connection with these Terms or the Services which is subject to disclosure under FOIA;
"Intellectual Property Rights"	means all patents, rights to inventions, utility models, copyright and related rights, trade-marks, service marks, trade, business and domain names, rights in trade dress or get-up, rights in goodwill or to sue for passing off, unfair competition rights, rights in designs, rights in computer software, database rights, topography rights, rights in data and confidential information (including know-how and trade secrets) and any other intellectual property rights, in each case whether registered or unregistered and including all applications for and renewals or extensions of such rights, and all similar or equivalent rights or forms of protection in any part of the world;
"LCIA Rules"	means the London Court of International Arbitration Rules;
"LSE"	means the London School of Economics & Political Science a company limited by guarantee (incorporated in England with company registration number 70527) and an exempt charity whose registered office address is at Houghton Street London WC2A 2AE;
"LSE Code of Research Conduct"	means LSE's code for the conduct of research which can be found here: https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/codResCon.pdf
"LSE Data Protection Policy"	means LSE's data protection policy which is to be found at: https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/datProPol.pdf
"LSE Information Classification Standard"	means LSE's guidance developed in accordance with the LSE Information Security Policy and the LSE Data Protection Policy which includes classification criteria and categories, which is found here: https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/infSecStalT.pdf
"LSE Information Security Policy"	means LSE's framework for information security which can be found here: https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/infSecPol.pdf
"LSE Materials"	has the meaning set out in Clause 3.3.6;
"LSE Procurement Policy and Procedures"	means LSE's policy for procurement which can be found here: https://info.lse.ac.uk/staff/divisions/Finance-Division/assets/documents/Procurement/PDFs/Procurement-Policy-and-Procedures-2023v1.pdf

"LSE Research Ethics Policy"	means LSE's policy for research ethics which can be found here: https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/resEthPolPro.pdf
"LSE Safeguarding in Research and International Activities policy"	means LSE's policy for safeguarding in relation to research and international activities which can be found here: https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/safResIntActPol.pdf
"LSE Safeguarding Policy"	means LSE's overarching policy for safeguarding which can be found here: https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/safPol.pdf
"Milestone"	means a milestone event in the performance of the Services (including the delivery of Outputs) signifying that certain elements of the Services should have been completed and delivered which (once achieved and approved by LSE) triggers a right for the Supplier to receive a payment for Services as set out in the Appointment Letter;
"New Supplier"	means any new provider of the Services, including LSE;
"Outputs"	means all documents, reports, inventions, databases, products and any other items or materials developed or created by the Supplier or its agents, contractors and employees for the purposes of or as part of or in relation to the Services, in any form or media (including digital media), including drawings, maps, plans, diagrams, designs, pictures, [films,] computer programs, data, data sets, specifications and reports (including drafts of any such things);
"Personal Data"	has the meaning given to that term in the Data Protection Act 2018 and the General Data Protection Regulation (EU) 2016/679);
"Principles and Responsibilities"	means the principles to which suppliers to LSE (including the Supplier) are required to adhere as set out in Annex 3;
"Process"	has the meaning given to that term in Data Protection Law and "Processed" and "Processing" and "Processor" shall be construed accordingly;
"Prohibited Act"	means: (a) to directly or indirectly offer promise or give a person working for LSE or FCDO a financial or other advantage: (i) to induce that person to perform improperly a relevant function or activity or induce that person to perform improperly a relevant function or activity; or (ii) reward that person for improper

	<p>performance of a relevant function or activity;</p> <p>(b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with the Contract;</p> <p>(c) an offence (i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); (ii) under legislation or common law concerning fraudulent acts; or (iii) defrauding, attempting to defraud or conspiring to defraud LSE or FCDO; or</p> <p>(d) any activity, practice or conduct which would constitute one of the offences listed under sub-clause (c) above if such activity, practice or conduct had been carried out in the United Kingdom;</p>
“Protective Measures”	<p>means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it;</p>
“Reasonable Measures”	<p>means using all reasonable endeavours to be expected of a professional and prudent supplier in the Supplier's industry to eliminate or minimise risk of Serious Misconduct as is reasonable and proportionate under the circumstances which may include:</p> <p>(a) clear and detailed policies and guidance for Supplier Personnel, and where appropriate, beneficiaries;</p> <p>(b) developing, implementing, maintaining and monitoring a safeguarding plan throughout the Term;</p> <p>(c) provision of regular training to Supplier Personnel and where appropriate, beneficiaries;</p> <p>(d) clear reporting lines and whistleblowing policies in place for Supplier Personnel and (where appropriate) beneficiaries;</p> <p>(e) maintaining detailed records of any allegations of Serious Misconduct and prompt reporting to LSE and (where relevant) FCDO (through its website at reportingconcerns@FCDO.gov.uk) and Appropriate Authorities of any such incidents;</p> <p>(f) any other Good Industry Practice measures (including any innovative solutions);</p>
"Recipient"	<p>means a party to the Contract which receives Confidential Information of the other party in its capacity as Disclosing Party;</p>

"Records"	means complete and accurate records and accounts of the operation of the Contract and the provision of the Services including in respect of financial information, costs, contract management, and compliance with applicable laws;
"Rectification Plan"	means a plan prepared by the Supplier designed to enable the Supplier to remedy its material remediable breach or failure to comply with the Contract containing information explaining the cause of the breach or failure, its effect on the fulfilment of the Services, the steps which the Supplier proposes to take to remedy the failure or breach, including proposed timetables for performance of rectification steps and any other information required by LSE;
"Relevant Requirements"	means all applicable laws relating to bribery, corruption and fraud, including the Bribery Act 2000 and any guidance issued by HMG Secretary of State for Justice pursuant to section 9 of the Bribery Act 2010;
"Relevant Transfer"	means a relevant transfer of an undertaking for the purposes of TUPE;
"Research Services"	means Services comprising the undertaking of research as designated by LSE;
"Security Policy"	means the HMG security policy (as updated periodically) which can be accessed at the location identified below (or such other location as may be notified to the Supplier from time to time): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/780851/Security-Policy-Contractors-Consultants-Suppliers-feb19.pdf ;
"Serious Misconduct"	means: (a) actual, attempted or threatened exploitation, abuse and harassment (including sexual abuse, exploitation and harassment) and whether or not such conduct would amount to a criminal offence in the United Kingdom or under the laws of the territory in which it takes place; (b) 'transactional sex' which shall include the exchange of money, employment, goods, or services for sex (including obtaining sexual favours) or any form of humiliating, degrading or exploitative behavior towards another person;
"Services"	means the services, including any Outputs, to be provided by the Supplier under these Terms as set out in the Appointment Letter; and (if applicable) Annex 2;
"Special Conditions"	means those special terms and conditions applicable to the Contract (if any) details of which (if applicable) are set out in

	Annex 5.
"Supplier"	means the person or entity specified as such in the Appointment Letter;
"Supplier Personnel"	means the individual or individuals engaged by the Supplier in the provision of the Services (whether as employee, worker, agent, contractor or otherwise, and including any employee, worker, agent, delivery chain partner or sub-contractor of the Supplier who is engaged in the provision of the Services);
"Term"	means the period commencing on the Commencement Date and expiring on the date specified as the end date in the Appointment Letter;
"Terms"	means these terms and conditions;
"Travel Policy"	means LSE IGC travel policy set out at: https://www.theigc.org/wp-content/uploads/2016/12/IGC-Travel-Policy.pdf (where applicable to the Contract);
"TUPE"	means the Transfer of Undertakings (Protection of Employment) Regulations 2006, as amended, and the Acquired Rights Directive 2001/23 EEC;
"UK Authorities"	means HMG bodies and agencies which have a responsibility for safeguarding, and for recording and investigating allegations of Serious Misconduct which may include FCDO, the National Crime Agency, United Kingdom Police, and social services;
"Use"	means reproduction, publication, issuing copies to the public, research activities and academic dissemination, in all media and all other uses required by LSE in order to meet its obligations under the FCDO Contract (but excluding uses for commercial exploitation).

1.2 Construction

In these Terms, the following rules apply:

- 1.2.1 a **person** includes a natural person, corporate or unincorporated body (whether or not having separate legal personality) and a reference to a party includes its personal representatives, successors or permitted assigns;
- 1.2.2 a reference to a statute or statutory provision is a reference to such statute or statutory provision as amended or re-enacted. A reference to a statute or statutory provision includes any subordinate legislation made under that statute or statutory provision, as amended or re-enacted;
- 1.2.3 a reference to a **Clause** is a reference to a clause in these Terms and a reference to an **Annex** is a reference to an annex to the Contract;

- 1.2.4 any phrase introduced by the terms **including, include, in particular** or any similar expression shall be construed as illustrative and shall not limit the sense of the words preceding those terms; and
- 1.2.5 (subject to the provisions of Clause 20.3) a reference to **writing** or **written** includes e-mails.

2. **COMMENCEMENT AND DURATION**

- 2.1 This Contract shall be deemed to have commenced on the Commencement Date and subject to provisions for earlier termination set out in Clause 16 shall expire at the end of the Term.

3. **SUPPLY OF SERVICES**

- 3.1 The Supplier shall from the Commencement Date and for the Term provide the Services to LSE in accordance with the terms of the Contract.
- 3.2 The Supplier shall meet any dates for performance of the Services specified in the Appointment Letter.
- 3.3 In providing the Services, the Supplier shall:
- 3.3.1 co-operate with LSE in all matters relating to the Services;
 - 3.3.2 perform the Services in accordance with Good Industry Practice;
 - 3.3.3 ensure that the Services and Outputs will conform with all requirements, and specifications set out in the Appointment Letter and these Terms;
 - 3.3.4 obtain and at all times maintain all necessary licences and consents, and comply with all applicable laws and regulations (including in regard to environmental, social and labour laws). In particular, the Supplier acknowledges LSE's commitment towards the prevention of slavery and/or human trafficking and therefore will ensure compliance with the Modern Slavery Act 2015;
 - 3.3.5 observe all health and safety laws and regulations:
 - (a) of the United Kingdom (and to the extent applicable) the European Union in respect of activities undertaken under this Contract in the United Kingdom;
 - (b) of the European Union in respect of activities undertaken under this Contract in the European Union; and
 - (c) applicable in any other jurisdiction where activities are undertaken under this Contract (or such higher standards as may be necessary effectively to ensure the health and safety of those Supplier Personnel engaged in the provision of the Services).
 - 3.3.6 hold all materials, equipment and tools, drawings, specifications and data supplied by LSE to the Supplier ("**LSE Materials**") in safe custody at its own risk, maintain LSE Materials in good condition until returned to LSE, and not dispose or use LSE Materials other than in accordance with LSE's written instructions or authorisation;
 - 3.3.7 not do or omit to do anything which may cause LSE to lose any licence, authority, consent or permission on which it relies for the purposes of conducting its business, and the Supplier acknowledges that LSE may rely or act on the Services;
 - 3.3.8 where the Services are performed in London, pay such personnel that are engaged in performing the Services, the London living wage in force from time to time;

- 3.3.9 procure that Supplier Personnel comply with reasonable security requirements of FCDO when they are attending FCDO premises;
 - 3.3.10 comply with FCDO policies notified to it in writing from time to time in respect of any Supplier Personnel who attend FCDO premises;
 - 3.3.11 comply with lawful instructions and reasonable directions of FCDO which are notified to the Supplier in writing by LSE from time to time;
 - 3.3.12 observe any security requirements that LSE may notify the Supplier as being applicable at any of LSE's premises.
- 3.4 The Supplier shall:
- 3.4.1 not engage in any business or professional activity which conflicts or could conflict with its obligations under the Contract;
 - 3.4.2 procure that no Supplier Personnel engage in any personal business or professional activity which conflicts (or could conflict) with any of its obligations under the Contract;
 - 3.4.3 notify LSE promptly on becoming aware of any actual or potential conflict of interest in relation to the Contract and provide recommendations for avoidance of such conflict (subject to any obligations of confidentiality) providing such information and assistance as may be reasonably necessary to ensure that any conflict is avoided or to resolve a conflict which has arisen;
 - 3.4.4 establish and maintain appropriate measures to avoid any conflict of interest arising in relation to the Contract and advise LSE on request of the detail of such measures;
 - 3.4.5 if requested to do so by LSE put in place Ethical Walls to ensure that no information relating to the Contract is shared with or made available to persons other than those directly engaged in providing Services;
 - 3.4.6 be entitled to supply services to third parties provided this does not prejudice the Supplier's ability to perform the Services in a timely and efficient matter or give rise to a conflict of interest.
- 3.5 In the event of any breach by the Supplier or Supplier Personnel of the provisions of Clause 3.4, LSE may terminate the Contract forthwith on written notice to the Supplier.
- 3.6 The Supplier will collaborate with LSE in raising awareness of IGC with international bodies, national governments and other governmental bodies as set out below:
- 3.6.1 all communication, promotional, marketing, influencing, lobbying or political engagement activity in respect of the product of the Services or Outputs shall explicitly and prominently acknowledge the funding to the Supplier from IGC and FCDO including through use where appropriate of FCDO's "*UK aid - from the British people*" logo in accordance with the Branding Guidelines (such use to be permitted in conjunction with other donor logos provided that acknowledgements in respect of IGC and FCDO are at least equal in prominence to those for other donors).
 - 3.6.2 the Supplier shall not use such LSE, IGC and FCDO brands in a way which misrepresents the Supplier's relationship with LSE, IGC or FCDO or may damage or jeopardise the reputation of LSE, IGC or FCDO.

- 3.6.3 if the Supplier is a corporate entity it shall not engage in communications, promotion, marketing, influencing, lobbying or political engagement activity [in respect of the subject matter of the Contract] at an institutional level or through a specialist policy or communications individual or team without the prior written approval of LSE.
- 3.7 The Supplier acknowledges that there is no intention to create a relationship of employer and employee between the Supplier and LSE (including where the Supplier is an individual or providing services through a service company) and that for the avoidance of doubt:
- 3.7.1 LSE will not (subject to any express provisions of the Appointment Letter and Clauses 3.8 and 3.9) make any provision for pension, sick pay, annual leave, maternity/paternity leave, maternity benefits, or pay income tax or national insurance contributions, (neither relating to employers nor employees) or similar payments or contributions on behalf of the Supplier and the Supplier must make all and any necessary arrangements in this respect.
- 3.7.2 the Supplier shall be solely responsible for the payment of any pensions, pensions contributions and employment benefits which may be due to Supplier Personnel and shall indemnify LSE against any claims arising from the non-payment or underpayment of such pensions, pensions contributions and employment benefits.
- 3.8 Where LSE considers that the provisions of Chapter 10 of Part 2 of the Income Tax (Earnings and Pensions) Act 2003 apply to any Supplier Personnel it will notify the Supplier in the Appointment Letter and make appropriate deductions of Employment Taxes. For the avoidance of doubt, the Fees payable to the Supplier are a gross sum and the Supplier will therefore receive a net sum, once deductions at the applicable rate have been made.
- 3.9 The Supplier will provide (and will procure that any relevant Supplier Personnel provide) to LSE promptly following a written request from LSE, full and accurate information to enable LSE to determine whether the provisions of Chapter 10 of Part 2 of the Income Tax (Earnings and Pensions) Act 2003 apply to such Supplier Personnel and so as to enable LSE to make any necessary deductions from Fees via payroll where LSE deems that such deductions are required following such determination.
- 3.10 Where one of the Parties proposes to modify the Services for any reason such Party shall notify the other Party in writing giving details of such proposed modifications and the Supplier shall within a reasonable period thereafter notify LSE in writing of the anticipated impact of such modifications (if any) on the Outputs, Milestones and the Charges. LSE shall consider such information and notify the Supplier in writing either:
- 3.10.1 that it approves such modifications (and any consequent changes to the Outputs and/or Milestones and/or Charges proposed by the Supplier) in which event the Supplier will undertake such modifications and any such proposed changes to the Outputs and/or Milestones and/or Charges shall be implemented; or
- 3.10.2 that it does not approve such modifications in which event the Supplier will not undertake such modifications and no changes to the Outputs, Milestones or Charges will be implemented.

4. LSE RIGHTS AND REMEDIES

- 4.1 LSE may:
- 4.1.1 in its discretion decide whether or not to use or publish any Outputs submitted by the Supplier;
- 4.1.2 copy, edit and change the format (but not the content) of Outputs in order to put summaries of such Outputs on its IGC website and in other IGC publications.

4.2 If the Supplier:

4.2.1 fails to perform the Services by the applicable dates for performance of the Services as specified in the Appointment Letter; or

4.2.2 provides Outputs which do not meet the requirements of the Appointment Letter or these Terms or are incomplete; or

4.2.3 (if applicable) provides Outputs which do not conform with Annex 2;

LSE may without limiting its other rights or remedies take one or more of the actions set out in Clause 4.3 below.

4.3 In the circumstances set out in Clause 4.2:

4.3.1 LSE may where such failure or default is (in the reasonable opinion of LSE) a material, irremediable failure or default take any of the actions set out below:

(a) terminate the Contract with immediate effect by giving written notice to the Supplier;

(b) refuse to accept any subsequent performance of the Services which the Supplier attempts to make;

(c) (in relation to Services other than Research Services) recover from the Supplier any costs incurred by LSE in obtaining substitute services from a third party;

(d) where LSE has paid in advance for Services that have not been provided by the Supplier, to have such sums refunded by the Supplier; or

(e) to claim damages for any additional costs, loss or expenses incurred by LSE which are in any way attributable to the Supplier's failure to meet such dates.

4.3.2 LSE may where such failure or default is (in the reasonable opinion of LSE) remediable:

(a) afford the Supplier in writing an opportunity (at the sole expense of the Supplier) to remedy the default or failure (and any damage resulting from such default or failure) in a timely manner in which event the Supplier shall do so within a timescale reasonably specified by LSE in writing (or if none in a timely manner);

(b) (where such default or failure is material) require the Supplier to prepare a Rectification Plan and (at LSE's option) LSE may suspend the Contract or the performance of all or part of the Services during the period in which the Rectification Plan is being prepared by the Supplier and considered by LSE.

4.4 Where LSE calls for a Rectification Plan the Supplier shall prepare and deliver such a plan to LSE as soon as possible and in any event within ten (10) Business Days of written notice from LSE and LSE shall promptly review the Rectification Plan and either:

4.4.1 notify the Supplier in writing that it is accepted (in which event the Supplier shall proceed to implement the Rectification Plan in accordance with its terms at no cost to LSE); or

4.4.2 notify the Supplier in writing that it is not accepted, giving reasons (which may include that it will take too long to implement, or it is insufficiently detailed to be capable of proper evaluation, or will not effectively remedy the default or failure) in which event LSE may require the Supplier to modify the Rectification Plan and undertake the process set out in this Clause 4.4 again or on written notice to the Supplier exercise its rights under Clause 4.3.1 notwithstanding the fact that the default or failure is remediable.

4.5 These Terms shall apply to any substituted or remedial services provided by the Supplier under Clause 4.4.

4.6 LSE's rights under the Contract are in addition to its rights and remedies implied by statute and common law, including the Supply of Goods and Services Act 1982.

5. **LSE'S OBLIGATIONS**

5.1 LSE shall:

5.1.1 if necessary, provide the Supplier with reasonable access at reasonable times to LSE's premises for the sole purpose of providing the Services; and

5.1.2 provide such information and supervision to the Supplier as the Supplier may reasonably request and LSE considers reasonably necessary for the purpose of providing the Services.

6. **CHARGES AND PAYMENT**

6.1 The Charges shall be the full and exclusive remuneration of the Supplier in respect of the performance of the Services. Unless otherwise agreed in writing by LSE, the Charges shall include every cost and expense of the Supplier directly or indirectly incurred in connection with the performance of the Services.

6.2 Where required by LSE (as set out in the Appointment Letter) the Supplier shall (where relevant subject to and conditional upon achieving the relevant Milestone and approval by LSE of the Output or Outputs related to such Milestone) issue invoices in respect of Services provided and Fees due in accordance with the Milestone timetable set out in the Appointment Letter or (if applicable) Annex 2 (or at such intervals otherwise as agreed with LSE). Each invoice submitted to LSE shall include the details agreed with LSE and such supporting information as may be required by LSE to verify the accuracy of the invoice (including details of the dates Services were provided, the period covered by the claim for payment and a brief description of the Services provided during such period). Subject to Clause 6.4 LSE shall pay (to a bank account nominated in writing by the Supplier) the invoiced amount no later than thirty (30) days from its receipt of a correct invoice submitted by the Supplier.

6.3 Where the Supplier is not required by LSE to issue invoices in respect of Fees, subject to Clause 6.4 LSE shall pay (to a bank account nominated in writing by the Supplier) the amounts specified in the Appointment Letter (or if applicable Annex 2) as being due in respect of the relevant approved Outputs, such payment to be no later than thirty (30) days after such approval is given.

6.4 If LSE disputes any invoice or other request for payment, LSE shall immediately notify the Supplier in writing. The parties shall negotiate in good faith to attempt to resolve the dispute promptly. The Supplier shall provide all such evidence as may be reasonably necessary to verify the disputed invoice or request for payment. Where only part of an invoice or payment is disputed, the undisputed amount shall be paid on the due date as set out in Clause 6.2 or 6.3 (as the case may be). For the avoidance of doubt, and subject to these Terms:

- 6.4.1 the Supplier's obligations to provide the Services shall not be affected by any payment dispute, including its obligations to provide the Services to which the payment dispute relates; and
- 6.4.2 the parties are be entitled to treat any unresolved dispute arising under Clause 6.4 as a "Dispute" for the purposes of this Contract.
- 6.5 The Supplier's invoices (where relevant) must be addressed to the department or division of LSE notified to the Supplier. LSE shall not be held responsible for delays in payment caused by the Supplier's failure to comply with LSE's invoicing instructions.
- 6.6 All amounts payable by LSE under the Contract are inclusive of all amounts which may be due in respect of any sales taxes (including value added tax) and goods and services taxes which may be chargeable for the time being.
- 6.7 If LSE fails to pay any amount properly due and payable by it under the Contract, the Supplier shall have the right to charge interest on the overdue amount at the rate of three per cent (3%) per annum above the base rate for the time being of The Royal Bank of Scotland plc accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgment. This Clause shall not apply to payments that LSE disputes in good faith as set out in Clause 6.4.
- 6.8 LSE reserves the right not to pay any amount due in respect of:
- 6.8.1 Services which are not provided in accordance with the requirements of the Appointment Letter or the terms and conditions of this Agreement; or
- 6.8.2 an Output which is either:
- (a) received by LSE more than 90 days after the final date by which such Output was due to be delivered to LSE;
 - (b) not compliant with the requirements set out in the Appointment Letter or the Terms or (if applicable) Annex 2 or as otherwise reasonably agreed by LSE; or
- 6.8.3 Services in respect of which the Supplier fails to submit a valid invoice to LSE (as required pursuant to Clause 6.2) within ninety (90) days of the date when such invoice is due to be submitted.
- 6.9 The Supplier will repay to LSE any overpayment of Charges made by LSE (including payments made in respect of Outputs and/or Services received late or not compliant with requirements as set out in Clause 6.8 above) within thirty (30) days of written notice from LSE to do so. LSE may, without limiting its other rights or remedies, set off any amount owed to it by the Supplier against any amount payable by LSE to the Supplier under the Contract or any other contract between the Supplier and LSE.
- 6.10 Payment of Charges shall (subject to Clause 6.11 below) be in the currency specified in the Appointment Letter.
- 6.11 In the event that the Charges include an amount by way of reimbursement of Expenses the Supplier will comply with the provisions of the Travel Policy and the Appointment Letter (or if applicable Annex 2) in respect of any travel expenses for which it seeks reimbursement and LSE shall pay such expenses which arise in a foreign currency at the exchange rate stated in OANDA (www.oanda.com) on the Friday immediately preceding the date on which the purchase was made or services acquired by the Supplier (or if this took place on a Friday at the rate specified on that

day). LSE's obligations in respect of the reimbursement of Expenses extend only to the cost of travel incurred in accordance with the Travel Policy.

6.12 In no event shall LSE pay by way of Charges an amount in excess of the budgeted amounts specified in either the Appointment Letter or (if applicable) Annex 2 (as the case may be).

7. **INTELLECTUAL PROPERTY RIGHTS**

7.1 Each party retains title to its Background IPR.

7.2 The Intellectual Property Rights in Outputs arising from the provision of Research Services shall vest in the Supplier.

7.3 The Supplier shall grant to LSE a worldwide non-exclusive, perpetual, irrevocable, royalty-free, assignable licence of the Intellectual Property Rights in:

7.3.1 Outputs arising from the provision of Research Services to Use such Outputs (with the power to grant a sub-licence to FCDO to Use such Outputs on the same terms as those granted to LSE under this Clause 7.3).

7.3.2 any Supplier's Background IPR which is embedded in or an integral part of any Outputs (whether through the provision of Research Services or other Services) to Use such Background IPR (with the power to grant a sub-licence to FCDO to Use such Background IP on the same terms as those granted to LSE under this Clause 7.3).

7.4 In respect of all Outputs (other than those arising from the provision of Research Services) the Supplier hereby assigns to LSE its entire right title and interest in all Intellectual Property Rights therein for the full period of such rights and any reversions, extensions or renewals thereof throughout the world.

7.5 The Supplier hereby warrants that:

7.5.1 (save for those extracts from third party works clearly identified by the Supplier to LSE) the content of the Outputs are original works and have not been published prior to their delivery to LSE;

7.5.2 the content of the Outputs is not and will not be defamatory and all statements made which purport to be factual statements are and will be true;

7.5.3 the Supplier has obtained (or will obtain) permission for the inclusion of such excerpts from the copyright owners of any excerpts from third party copyright works which are incorporated into any Outputs and has acknowledged (or will acknowledge) their sources in the Outputs.

7.6 The Supplier shall obtain waivers of all moral rights in the Outputs (other than those arising from the provision of Research Services), to which any individual is now or may be at any future time entitled under Chapter IV of Part I of the Copyright Designs and Patents Act 1988 or any similar provisions of law in any jurisdiction.

7.7 The Supplier shall, promptly at LSE's request, do (or procure to be done) all such further acts and things and the execution of all such other documents as LSE may from time to time require for the purpose of securing for LSE the full benefit of the Contract.

7.8 All Intellectual Property Rights in LSE Materials are the exclusive property of LSE and all Intellectual Property Rights in FCDO Information are the exclusive property of FCDO.

8. DATA PROTECTION AND FREEDOM OF INFORMATION

Data Protection:

- 8.1 To the extent that the Supplier is a data Controller (within the meaning of any Data Protection Law) the Supplier shall:
 - 8.1.1 ensure that the provision of any Personal Data to LSE is in accordance with the provisions of Data Protection Law;
 - 8.1.2 ensure that the use by LSE of any Personal Data provided by the Supplier for the purposes of or in connection with the Services shall not put LSE in breach of any Data Protection Law;
 - 8.1.3 notify LSE of any restrictions that may exist in relation to the use of Personal Data provided by the Supplier at the point such Personal Data is submitted to LSE.
- 8.2 If at any point in the delivery of the Services the Supplier is processing Personal Data as a data Processor under Data Protection Law the parties shall enter into a separate agreement as required by Data Protection Law.
- 8.3 The provisions of Annex 4 (a) shall apply in the event that:
 - 8.3.1 LSE transfers Personal Data to the Supplier in the course of this Agreement where the Supplier is based outside of the European Economic Area (EEA);
 - 8.3.2 the Supplier is based in the EEA and transfers Personal Data to a third party in the course of the provision of Services under this Agreement.
- 8.4 Where the Supplier is based outside of the EEA the Supplier will use all reasonable endeavours to avoid the use of Personal Data in Outputs and will where necessary take steps to anonymise information about living individuals in Outputs and when transferring Personal Data to third parties. If it is not possible for the Supplier to anonymise the Personal Data, it will ensure that any transfer of such Personal Data complies with the provisions of the LSE Data Sharing Minimum Standards attached at Annex 4 (c).

Freedom of Information:

- 8.5 The Supplier shall assist and cooperate with LSE to enable it to comply with its obligations under FOIA. In particular, the Supplier shall:
 - 8.5.1 transfer to LSE all requests for Information pursuant to FOIA that it receives as soon as practicable and in any event within two (2) Business Days of receiving the request; and
 - 8.5.2 provide LSE with assistance in complying with requests for Information received pursuant to FOIA including the provision of Information held on behalf of LSE and covered by the request in the form that LSE requires. Such assistance shall be provided promptly and in any event within three (3) Business Days of LSE making a request to the Supplier to provide any necessary Information or assistance.
- 8.6 As soon as reasonably practicable following receipt of a request for assistance under sub-clause 8.5, the Supplier shall:
 - 8.6.1 notify LSE whether it holds the Information covered by the request on behalf of LSE, provided that LSE shall not be obliged to display a copy of the request to the Supplier;

- 8.6.2 if it does so hold the Information, provide all such Information covered by the request to LSE; and
- 8.6.3 demonstrate to the satisfaction of LSE the steps taken by the Supplier to comply with its obligations under this sub Clause.
- 8.7 In no event shall the Supplier respond directly to a request for Information unless expressly authorised to do so by LSE.
- 8.8 The Supplier acknowledges that LSE may, and/or may be obliged to, disclose any information received from the Supplier including any Commercially Sensitive Information.
- 8.9 Subject to Clause 8.11.1 LSE shall consult with the Supplier prior to responding to any request under FOIA for Commercially Sensitive Information received by LSE from the Supplier.
- 8.10 LSE shall take account of any response received from the Supplier pursuant to Clause 8.9 but, notwithstanding this, LSE shall be responsible for determining in its absolute discretion and, notwithstanding any other provision in this Contract or any other contract, whether the Commercially Sensitive Information and/or any other Information is exempt from disclosure in accordance with the provisions of FOIA.
- 8.11 The Supplier acknowledges that LSE may be obliged under FOIA to disclose information concerning the Supplier or the Services:
 - 8.11.1 in certain circumstances without consulting the Supplier; or
 - 8.11.2 following consultation with the Supplier and having taken its views into account, provided always that where Clause 8.11.1 applies LSE shall take reasonable steps, where appropriate, to give the Supplier advance notice, or failing that, to draw the disclosure to the Supplier's attention after any such disclosure.
- 8.12 In complying with the obligations of this Clause 8, each party agrees that it shall at all times act in good faith and the Supplier undertakes to do nothing to prevent LSE from complying with its obligations under FOIA.

9. **SUPPLIER PERSONNEL**

- 9.1 The Supplier shall ensure that all Supplier Personnel have the appropriate skills, qualifications, training and experience to carry out those parts of the Services for which they are responsible with all due care, skill and diligence and in a professional and workmanlike manner, and the Supplier shall ensure that Supplier Personnel are provided in sufficient number to ensure that the Supplier's obligations are fulfilled in accordance with the Contract.
- 9.2 The Supplier shall use its reasonable endeavours to ensure the continuity of Supplier Personnel assigned to perform the Services. If the Supplier is required to replace Supplier Personnel it shall provide a replacement of comparable skill, qualification and experience as soon as possible, and any required handover or period of familiarisation shall be at the expense of the Supplier.
- 9.3 The Supplier acknowledges that in relation to Supplier Personnel it is responsible for:
 - 9.3.1 their acts and omissions;
 - 9.3.2 carrying out appropriate risk assessments with regard to the delivery of Services;

- 9.3.3 providing adequate information, instruction, training and supervision;
- 9.3.4 ensuring their health, safety, security and wellbeing (and the security of their property while they are engaged in providing Services); and
- 9.3.5 having appropriate emergency procedures in place to prevent or mitigate the risk of damage to the health, safety, security and wellbeing of Supplier Personnel (and of security of their property while they are engaged in providing Services).

9.4 The Supplier undertakes to ensure that Supplier Personnel who are required to undertake Services in the United Kingdom or another country (other than their country of residence) comply with all applicable legal requirements for entry to the United Kingdom or such other country including obtaining such entry visas as may be required from time to time and the Supplier undertakes if so requested by LSE to provide evidence of its compliance with such requirements.

10. **EQUITY, DIVERSITY AND INCLUSION**

10.1 The Supplier shall, and shall procure that the Supplier Personnel, comply with any and all applicable anti-discrimination legislation, including:

10.1.1 (where applicable) the Equality Act 2010]; and

10.1.2 the International Development (Gender Equality) Act 2014 or other relevant or equivalent legislation.

10.2 The Supplier will:

10.2.1 in the provision of the Services have due regard to the advancement of equal opportunities and promotion of good relations between people (including those with and without protected characteristics);

10.2.2 provide evidence to LSE, on written request, of the Supplier's compliance with applicable anti-discrimination legislation in provision of the Services (including in the Supplier's employment practices), in order to satisfy LSE that the Supplier takes all reasonable steps to promote equity, diversity and inclusion in provision of the Services and in the Supplier's work environment; and

10.2.3 where the Supplier is domiciled in the United Kingdom or engaging employees or personnel in Great Britain it shall adhere to current relevant codes of practice published by the Equality and Human Rights Commission, ensuring compliance by Supplier Personnel and suppliers engaged in the performance of the Services.

10.3 The Supplier will indemnify LSE against any claims from FCDO under the FCDO Contract arising from a Default by the Supplier in its compliance with the terms of this Clause 10.

11. **NO TRANSFER OF EMPLOYEES**

11.1 It is the understanding of the parties that TUPE does not apply on the commencement of the provision of the Services by the Supplier under the Contract.

11.2 The Supplier agrees to arrange Supplier Personnel in relation to the provision of the Services in such a way that no individual at any time:

- (a) forms part of an organised grouping of employees which has as its principal purpose the provision of all or part of the Services; or

- (b) is wholly or mainly assigned to the provision of all or part of the Services.
- 11.3 The Supplier and LSE agree that on termination of all or part of the Contract, TUPE will not apply so as to transfer the employment of any Supplier Personnel to a New Supplier.
- 11.4 If any Supplier Personnel argue that they should have transferred to a New Supplier under TUPE, the New Supplier will refuse to employ the Supplier Personnel.
- 11.5 The Supplier will indemnify LSE and/or the New Supplier immediately on demand for any costs, losses, expenses (including the costs of LSE and/or the New Supplier's advisors including legal advisors), awards or orders made by a tribunal or court or otherwise paid which relate to:
- (a) any claim arising from the employment or termination of employment of any Supplier Personnel at any time, including after termination of all or part of the Contract;
 - (b) any claim brought by any Supplier Personnel (or on his or her behalf by a trade union or other representative) as a result of a New Supplier's actions under Clause 11.2 above;
 - (c) a claim of any kind from anyone other than Supplier Personnel who argues that they should have transferred to a New Supplier under TUPE on termination of all or part of the Contract; and
 - (d) any claim brought by any Supplier Personnel (or on his or her behalf by a trade union or other representative) as a result of any failure to comply with any obligation to inform and consult under TUPE or any equivalent or similar law.
- 11.6 In return, LSE will and will take reasonable steps to procure that the New Supplier will:
- (a) as soon as it can after becoming aware of any relevant claim (or coming to the conclusion that a claim is likely to occur), make the Supplier aware of the situation and give the Supplier a written summary of any relevant facts; and
 - (b) do anything that the Supplier reasonably asks of LSE or the New Supplier in relation to the claim, including resisting or settling the claim, subject to LSE or the New Supplier being allowed to employ its own legal advisors to carry out those tasks and the Supplier meeting any costs or expenses that need to be paid as a result of that work.

12. RECORD KEEPING, INFORMATION AND AUDIT

- 12.1 The Supplier shall:
- 12.1.1 create, keep and maintain Records in accordance with Good Industry Practice and applicable laws during the Term and for seven (7) years after its expiry or termination;
 - 12.1.2 during normal business hours of the Supplier afford LSE (or its authorised agents or representatives) access to the Records at the Supplier's premises or (at the option of LSE) provide copies of such Records to LSE in a format reasonably acceptable to LSE from time to time during the Term and thereafter for the period specified in Clause 12.1.1.
- 12.2 LSE shall be entitled to pass details of such Records to FCDO and both LSE and FCDO (and FCDO's agents) shall be entitled to review such Records for the purposes of:
- 12.2.1 verifying the accuracy of information provided as required by the Contract, the Charges and any other amounts payable under this Contract;
 - 12.2.2 verifying the costs of the Supplier in connection with the provision of the Services;

- 12.2.3 verifying the Supplier's compliance with the applicable laws;
 - 12.2.4 identifying or investigating an actual or suspected Prohibited Act, impropriety or accounting mistake or any breach or threatened breach of security and in these circumstances LSE shall have no obligation to inform the Supplier of the purpose or objective of its investigations;
 - 12.2.5 obtaining such information as is necessary to fulfil LSE's obligations to FCDO under the terms of the FCDO Contract;
 - 12.2.6 reviewing the Supplier's quality management systems (including any quality manuals and procedures) and compliance with any standards referred to in the Contract or applicable to the provision of the Services.
- 12.3 The Supplier undertakes to co-operate with and provide reasonable assistance to LSE in connection with any request for copies of Records or inspection of Records and for such purposes to provide promptly on request:
- 12.3.1 information reasonably requested by LSE;
 - 12.3.2 access to sites controlled by the Supplier; and
 - 12.3.3 access to relevant Supplier Personnel.
- 12.4 The parties shall each bear their own costs and expenses incurred in regard to compliance with their obligations under this Clause 12 unless an audit reveals a Default by the Supplier in which case LSE is entitled to recover from the Supplier its costs of carrying out such audit (and any costs recoverable by FCDO from LSE under the FCDO Contract in connection with such audit).
- 13. INDEMNITY AND INSURANCE**
- 13.1 The Supplier shall indemnify LSE and keep LSE indemnified on demand and in full against all costs, expenses, damages and losses (whether direct or indirect), including any interest, fines, legal and other professional fees and expenses awarded against or incurred or paid by LSE as a result of or in connection with:
- 13.1.1 any claim made against LSE by a third party arising out of, or in connection with, the supply of the Services, to the extent that such claim arises out of the breach, negligent performance or failure or delay in performance of the Contract by the Supplier, its employees, agents or subcontractors; and
 - 13.1.2 any claim brought against LSE for actual or alleged infringement of a third party's Intellectual Property Rights arising out of, or in connection with, the receipt, use or supply of the Services or any Deliverable.
- 13.2 Where applicable, the Supplier shall be responsible for and shall indemnify LSE against all Employment Taxes, where such recovery is not prohibited by law. The Supplier shall further indemnify LSE against all reasonable costs, expenses and any penalty, fines and interest incurred or payable by LSE in connection with or in consequence of any liability for such Employment Taxes. In this regard, such liability for Employment Taxes shall be deemed to arise and LSE shall be deemed to be obliged to pay an amount, if it receives a written demand from HM Revenue and Customs.
- 13.3 The Supplier shall be fully responsible for and shall indemnify LSE for and in respect of any liability arising from any employment-related claim or any claim based on worker status (including

reasonable costs and expenses) brought by any Supplier Personnel against LSE arising out of or in connection with the provision of the Services under the Contract.

- 13.4 For the duration of the Contract and for a period of six (6) years thereafter, the Supplier shall maintain in force with a reputable insurance company insurance at a level which it considers reasonably necessary to cover the liabilities that may arise under or in connection with the Contract which it is usual prudent and professional to insure in relation to an organisation of the type of the Supplier in accordance with best practice and applicable laws, such insurances to include:
- 13.4.1 risks which LSE specifically asks the Supplier in writing to take out prior to the Commencement Date; and
- 13.4.2 risks in respect of Supplier Personnel including death, injury, disablement and the cost of emergency medical treatment.
- 13.5 The Supplier shall on LSE's request produce both the insurance certificate giving details of its cover and the receipt for the current year's premium in respect of such insurance.

13.6 This Clause 13 shall for the avoidance of doubt survive termination of the Contract.

14. **CONFIDENTIALITY**

- 14.1 Each party in its capacity as Recipient shall:
- 14.1.1 keep in strict confidence all Confidential Information of the Disclosing Party;
- 14.1.2 not use such Confidential Information for any purpose other than in order to exercise its rights and fulfil its obligations under the Contract;
- 14.1.3 only disclose such Confidential Information to such of its employees, agents and consultants as need to know the same for the purpose of discharging the Recipient's obligations under the Contract or as agreed in writing by the Disclosing Party;
- 14.1.4 ensure that those employees, agents or consultants to whom it discloses such Confidential Information are subject to obligations of confidentiality corresponding to those which bind the Recipient under this Clause 14;
- 14.1.5 only copy reduce to writing or otherwise record such Confidential Information except as strictly necessary in order to exercise its rights and fulfil its obligations under the Contract.
- 14.2 The obligations in this Clause 14 shall not apply in relation to:
- 14.2.1 information which is or becomes public knowledge other than as a result of a breach of Clauses 14.1 or 14.2;
- 14.2.2 information which is made available to the Recipient on a non-confidential basis prior to disclosure by or on behalf of the Disclosing Party;
- 14.2.3 information which is made available to the Recipient on a non-confidential basis by a third party who is not under any confidentiality obligation in respect of such information;
- 14.2.4 information developed independently by the Recipient without any access to the Confidential Information of the other party.
- 14.3 A party may disclose Confidential Information of the other to the extent required by:
- 14.3.1 an order of a court of competent jurisdiction or regulatory judicial governmental or similar body;

14.3.2 the rules of any listing authority or stock exchange on which its shares are listed or traded;
or

14.3.3 the laws or regulations of a country to which such party is subject.

14.4 The Supplier acknowledges that LSE may pursuant to the terms of the FCDO Contract be obliged to disclose Confidential Information of the Supplier to FCDO which may itself (if it deems such disclosures necessary or appropriate in the course of carrying out its public functions) disclose such Confidential Information to other HMG agencies institutions or appointed bodies or to advisors of FCDO or such other HMG agencies, institutions or appointed bodies provided that FCDO procures that recipients of such disclosures enter into confidentiality undertakings in respect of such Confidential Information.

14.5 This Clause 14 shall survive termination of the Contract.

15. **COMPLIANCE**

Code of Conduct:

15.1 The Supplier will comply with the Principles and Responsibilities and in the event that LSE informs the Supplier in writing either before or during the Term that the Supplier falls within the definition of a Compliance Level 2 Supplier then the Supplier shall forthwith thereafter for such period during the Term as LSE shall specify, comply with the Code of Conduct and the monitoring requirements set out in the Code of Conduct. For the purposes of this Clause 15.1 an email communication shall not constitute a notice under Clause 20.3.

15.2 The Supplier will indemnify LSE against any claims from FCDO under the FCDO Contract arising from a Default by the Supplier in its compliance with the terms of Clause 15.1.

Bribery and Corruption:

15.3 The Supplier will comply with all applicable laws, statutes, regulations and codes relating to anti-bribery and anti-corruption in its jurisdiction including the Bribery Act 2010 and will not engage in any activity, practice or conduct which would constitute a Prohibited Act.

15.4 The Supplier will:

15.4.1 not make any payments, or offer or transfer anything of value, to any government official or government employee, to any political party official or to any other third party and will promptly report to LSE any request or demand for any undue financial or other advantage of any kind received by the Supplier in connection with the performance of the Contract;

15.4.2 not do or suffer anything to be done which would cause LSE, FCDO or any FCDO Personnel to contravene or incur any liabilities in respect of any Relevant Requirements;

15.4.3 establish, maintain and enforce policies and procedures adequate to ensure compliance with the Relevant Requirements and prevent the occurrence of a Prohibited Act;

15.4.4 keep appropriate records of its compliance with the obligations in this Clause 15 and make sure records are available to LSE on request; and

15.4.5 ensure that any person associated with the Supplier who is performing services in connection with the Contract does so only on the basis of a written contract which imposes on and secures from such person terms equivalent to those imposed on the Supplier in this Clause 15.

15.5 The Supplier shall notify LSE in writing if it:

- (a) becomes aware of any breach of Clauses 15.3 or 15.4;
- (b) has reason to believe that any Supplier Personnel have been subject to an investigation or prosecution which relates to a Prohibited Act, or have been debarred or suspended or deemed ineligible for participation in any government procurement programme or contract on the grounds of having committed a Prohibited Act, or have received a demand for any undue financial or other advantage of any kind in connection with the performance of the Contract; or
- (c) has any credible suspicion of or evidence of fraud bribery corruption or other financial irregularity or impropriety which relates to the Contract or the provision of the Services.

15.6 In the event of any breach of Clauses 15.3 or 15.4 or any act by any Supplier Personnel which would amount to a breach of this Clause 15 LSE shall, without prejudice to any other rights it may possess, be at liberty immediately to terminate the Contract and to recover from the Supplier the amount of any loss or damage suffered by LSE resulting from such termination, as well as the amount or value of any unlawful payment made or to recover any other loss derived from the breach of Clauses 15.3 or 15.4 whether or not the Contract is terminated.

Prevention of terrorism:

15.7 The Supplier:

15.7.1 will ensure that to the best of its knowledge funding provided by LSE under the Contract (and any other funding received by the Supplier from United Kingdom sources) is not made available whether directly or indirectly to persons groups or entities listed in accordance with the European Council Regulation EC/2580/2001 (as amended) and/or the Terrorism (United Nations Measures) Order 2009 of the United Kingdom or contravene the provisions of such terrorism legislation (or any subsequent applicable legislation) or any equivalent terrorism legislation relevant to its jurisdiction;

15.7.2 warrants and represents that neither it nor to the best of its belief Supplier Personnel have at any time prior to the Commencement Date appeared on the HMG Home Office Proscribed Terrorist Organisation List;

15.7.3 will notify LSE immediately in writing if it becomes aware of a breach of this Clause 15.7 or has reason to believe that any Supplier Personnel have been subject to investigation or prosecution relating to an infringement of this Clause 15.7 or have been listed by a government department or agency as having been debarred or suspended or otherwise deemed ineligible for participation in government procurement programmes or contracts.

15.8 In the event that the Supplier or (with or without the knowledge of the Supplier) any Supplier Personnel breaches any provisions of Clause 15.7 or commits any offence under the Terrorism Act 2000 in relation to the Contract or any agreement with HMG LSE shall be entitled to terminate the Contract with immediate effect by written notice to the Supplier and recover the amount of any loss resulting from such termination or to recover any other loss derived from the breach of Clause 15.7 whether or not the Contract is terminated.

Environment:

- 15.9 The Supplier will provide the Services in accordance with applicable national and international environmental laws (taking account of LSE's environmental operations policy and the sustainable development provisions of the International Development Act 2002) and shall notify LSE promptly on becoming aware of any materially adverse changes in the environmental impact of its activities in connection with the Contract.

General security requirements:

- 15.10 The Supplier shall comply with any relevant obligations arising in respect of FCDO Information under the Official Secrets Acts 1911 - 1989.
- 15.11 The Supplier shall in relation to primary or secondary research data either meet the LSE Information Security Policy and classify such data by reference to the LSE Information Classification Standard or adhere to institutional policies which guarantee at least the same level of security as may be notified by the Supplier to LSE from time to time.
- 15.12 The Supplier shall (if required to do so in writing by LSE) produce in writing and submit to LSE for approval a security plan in respect of data (which plan LSE shall in writing either approve or require modifications in which event the Supplier shall make such modifications and re-submit such plan to LSE for approval in accordance with this Clause 15.12).
- 15.13 The Supplier shall (at its sole cost) take reasonable measures to avoid the introduction of Malware into its computer systems and network which may adversely affect its performance of its obligations under the Contract or lead to contamination of computer systems and networks of LSE or FCDO.
- 15.14 The Supplier undertakes:
- 15.14.1 not to delete or remove any proprietary notices contained with any FCDO Information in its possession;
 - 15.14.2 not to store, copy, disclose or use FCDO Information except as necessary for the performance by the Supplier of its obligations under this Contract or as expressly authorised by LSE;
 - 15.14.3 to make available on written demand a copy of any FCDO Information in its possession to FCDO or LSE in a format specified by FCDO or LSE (as the case may be);
 - 15.14.4 to preserve the integrity of FCDO Information in its possession and prevent its loss or corruption, perform back-ups thereupon and store them off-site and in the event of any loss or corruption thereof notify LSE without delay and take all appropriate steps to restore or procure the restoration of such FCDO Information at its sole cost;
 - 15.14.5 to ensure that any FCDO Information in its possession is held on a system under its control which meets the Security Policy and any other security requirements notified by LSE to the Supplier in respect thereof.

LSE Research Ethics Policy and LSE Code of Research Conduct

- 15.15 If the Supplier is providing Research Services then the Supplier undertakes to comply with the LSE Research Ethics Policy and the LSE Code of Research Conduct or, where applicable, to adhere to its own research ethics policy and code of research conduct or similar, provided that these documents contain standards that are no less rigorous than those of LSE.

Procurement

- 15.16 The Supplier undertakes to comply with the LSE Procurement Policy and Procedures or, where applicable, to adhere to its own procurement policies and procedures, provided that these documents contain standards that are no less rigorous than those of LSE.

16. **TERMINATION**

- 16.1 Without limiting its other rights or remedies, LSE may terminate the Contract with immediate effect by giving written notice to the Supplier if:
- 16.1.1 the Supplier commits a material irremediable breach of the Contract;
 - 16.1.2 the Supplier has failed to remedy a material remediable breach in accordance with a Rectification Plan previously approved by LSE;
 - 16.1.3 the Supplier commits a material or persistent breach of the Contract and (if such a breach is remediable) fails to remedy that breach within thirty (30) days of receipt of notice in writing from LSE of the breach;
 - 16.1.4 the Supplier suspends, or threatens to suspend, payment of its debts or is unable to pay its debts as they fall due or admits inability to pay its debts or (being a company) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986 or (being an individual) is deemed either unable to pay its debts or as having no reasonable prospect of so doing, in either case, within the meaning of Section 268 of the Insolvency Act 1986 or (being a partnership) has any partner to whom any of the foregoing apply;
 - 16.1.5 the Supplier commences negotiations with all or any class of its creditors with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with its creditors other than (where a company) for the sole purpose of a scheme for a solvent amalgamation of the Supplier with one or more other companies or the solvent reconstruction of the Supplier;
 - 16.1.6 a petition is filed, a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of the Supplier (being a company) other than for the sole purpose of a scheme for a solvent amalgamation of the Supplier with one or more other companies or the solvent reconstruction of the Supplier;
 - 16.1.7 the Supplier (being an individual) is the subject of a bankruptcy petition order;
 - 16.1.8 a creditor or encumbrancer of the Supplier attaches or takes possession of, or a distress, execution, sequestration or other such process is levied or enforced on or sued against, the whole or any part of its assets and such attachment or process is not discharged within 14 days;
 - 16.1.9 an application is made to court, or an order is made, for the appointment of an administrator or if a notice of intention to appoint an administrator is given or if an administrator is appointed over the Supplier (being a company);
 - 16.1.10 a floating charge holder over the assets of the Supplier (being a company) has become entitled to appoint or has appointed an administrative receiver;
 - 16.1.11 a person becomes entitled to appoint a receiver over the assets of the Supplier or a receiver is appointed over the assets of the Supplier;
 - 16.1.12 any event occurs, or proceeding is taken, with respect to the Supplier in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned in Clause 16.1.4 to Clause 16.1.11 (inclusive);
 - 16.1.13 the Supplier suspends or threatens to suspend, or ceases or threatens to cease to carry on, all or a substantial part of its business; or

16.1.14 the Supplier (being an individual) dies or, by reason of illness or incapacity (whether mental or physical), is incapable of managing his own affairs or becomes a patient under any mental health legislation.

16.2 Without limiting its other rights or remedies, LSE may terminate the Contract by giving the Supplier at least thirty (30) days prior written notice.

17. CONSEQUENCES OF TERMINATION

17.1 On termination of the Contract for any reason:

17.1.1 the Supplier shall immediately deliver to LSE all Outputs and the product of all Services up to the date of termination whether or not then complete, and return all LSE Materials. If the Supplier fails to do so, then LSE may enter the Supplier's premises and take possession of the Outputs and/or the product of the Services and/or the LSE Materials (as the case may be). Until the Outputs and/or the product of the Services and/or the LSE Materials (as the case may be) have been returned or delivered, the Supplier shall be solely responsible for their safe keeping and will not use them for any purpose unconnected with the Contract;

17.1.2 (subject to any right of set off which LSE may have against the Supplier in respect of sums due from the Supplier to LSE) LSE will pay such sums which may be due and payable by way of Charges to the Supplier on termination of the Agreement subject to the Supplier having submitted all relevant information and (if applicable) invoices necessary for such payment to be made;

17.1.3 the accrued rights, remedies, obligations and liabilities of the parties as at termination, including the right to claim damages in respect of any breach of the Contract which existed at or before the date of termination shall not be affected by such termination; and

17.1.4 Clauses which expressly or by implication have effect after termination shall continue in full force and effect.

18. MULTI-TIERED DISPUTE RESOLUTION PROCEDURE

18.1 If a Dispute arises then the parties shall follow the procedure set out in this Clause:

18.1.1 either party may serve on the other a Dispute Notice setting out the nature and full particulars of the Dispute together with relevant supporting documents. On service of the Dispute Notice, a nominated representative of the Supplier and a nominated representative of LSE shall attempt in good faith to resolve the Dispute;

18.1.2 if the nominated representative of the Supplier and the nominated representative of LSE are for any reason unable to resolve the Dispute within thirty (30) days of service of the Dispute Notice, the Dispute shall be referred to a senior representative of the Supplier and a senior representative of LSE who shall attempt in good faith to resolve it; and

18.1.3 if the senior representative of the Supplier and the senior representative of LSE are for any reason unable to resolve the Dispute within thirty (30) days of it being referred to them, the parties will attempt to settle it by mediation in accordance with the CEDR Model Mediation Procedure. Unless otherwise agreed between the parties, the mediator shall be nominated by CEDR Solve. To initiate the mediation, a party must serve notice in writing ("**ADR notice**") to the other party to the Dispute, requesting a mediation. A copy of the ADR notice should be sent to CEDR Solve. The mediation will start not later than thirty (30) days after the date of the ADR notice.

18.2 The commencement of mediation shall not prevent the parties commencing or continuing court proceedings or other dispute resolution procedures in relation to the Dispute under Clauses 20.9 and 20.10 and which Clauses shall apply at all times.

19. **SAFEGUARDING**

- 19.1 The Supplier undertakes to comply with the LSE Safeguarding policy and, if the Supplier is providing Research Services or is based overseas, then the Supplier also undertakes to comply with the LSE Safeguarding in Research and International Activities policy. Where applicable, the Supplier may adhere to its own safeguarding policies or similar, provided that these documents contain standards that are no less rigorous than those of LSE and that the Supplier complies with the remaining provisions of this clause 19.
- 19.2 The Supplier shall take all Reasonable Measures to prevent Serious Misconduct by the Supplier Personnel or any other persons engaged and controlled by it to perform any activities under the Contract and shall have in place at all times robust procedures which enable the reporting by Supplier Personnel and beneficiaries of any such Serious Misconduct, illegal acts and/or failures by Supplier Personnel to investigate such reports.
- 19.3 The Supplier shall take all Reasonable Measures to ensure that Supplier Personnel do not engage in sexual activity with any person under the age of 18, regardless of the local age of majority or age of consent or any mistaken belief held by Supplier Personnel as to the age of the relevant person.
- 19.4 The Supplier shall promptly report in writing any complaints, concerns and incidents regarding Serious Misconduct or any attempted or threatened Serious Misconduct by any Supplier Personnel to LSE (and where required by LSE in writing also to report to FCDO and where appropriate to Appropriate Authorities) and (where the Supplier is domiciled in the United Kingdom) the Supplier shall (where appropriate) report such matters to UK Authorities.
- 19.5 The Supplier shall fully investigate and document all actual, alleged or possible cases of Serious Misconduct and shall take appropriate corrective action to reduce the risk and/or eliminate Serious Misconduct being committed by Supplier Personnel (which may include disciplinary action, termination of contracts etc.), such investigations and actions to be reported to LSE and Appropriate Authorities as soon as is reasonably practicable.
- 19.6 The Supplier shall not engage as Supplier Personnel for the purposes of the Services any person whose previous record or conduct which is known to the Supplier (or which ought to be known by a diligent supplier undertaking appropriate checks) indicates that they are unsuitable to perform the Services and/or where they represent an increased and unacceptable risk of committing Serious Misconduct.
- 19.7 The Supplier shall comply with all applicable laws, legislation, codes of practice and government guidance in the United Kingdom and additionally, in the territories where the Services are being performed, relevant to safeguarding and protection of children and vulnerable adults, which the Supplier acknowledges may include vetting of Supplier Personnel by the United Kingdom Disclosure and Barring Service in respect of any regulated activity performed by the Supplier Personnel (as defined by the Safeguarding Vulnerable Groups Act 2006 (as amended)) and/or vetting by a local equivalent service. Where LSE reasonably believes that there is an increased risk to safeguarding in the performance of the Services, the Supplier shall comply with any reasonable request by LSE for additional vetting to be undertaken.
- 19.8 Failure by the Supplier to:
- 19.8.1 put in place preventative measures to eliminate and/or reduce the risk of Serious Misconduct; or
- 19.8.2 fully investigate allegations of Serious Misconduct; or

- 19.8.3 report any complaints to LSE and where relevant UK Authorities and/or Appropriate Authorities;

shall be a material Default of this Contract and shall entitle LSE to terminate the Contract on written notice with immediate effect.

20. GENERAL

- 20.1 **Matters beyond control:** Neither party shall be liable to the other as a result of any delay or failure to perform its obligations under the Contract if and to the extent such delay or failure is caused by an event or circumstance which is beyond the reasonable control of that party which by its nature could not have been foreseen by such a party or if it could have been foreseen was unavoidable. If such event or circumstances prevent the Supplier from providing any of the Services for more than six (6) weeks, LSE shall have the right, without limiting its other rights or remedies, to terminate the Contract with immediate effect by giving written notice to the Supplier.

20.2 Assignment and subcontracting:

- 20.2.1 The Supplier shall not assign, transfer, charge, or deal in any other manner with all or any of its rights or obligations under the Contract without the prior written consent of LSE (such consent not to be unreasonably withheld or delayed).

- 20.2.2 The Supplier may sub-contract obligations to sub-contractors provided that it:

- (a) remains responsible for all acts and omissions of its sub-contractors (including any sub-sub-contractors) as though they were its own; and
- (b) imposes on its sub-contractors obligations equivalent to those imposed on the Supplier under the Contract.

- 20.2.3 LSE may at any time assign, transfer, charge, subcontract novate or deal in any other manner with all or any of its rights under the Contract and may novate, subcontract or delegate in any manner any or all of its obligations under the Contract to any third party or agent.

20.3 Notices:

- 20.3.1 Any notice or other communication required to be given to a party under or in connection with the Contract shall be in writing and sent by e-mail to the other party's e-mail address as set out in the Appointment Letter (or as otherwise notified by the other party from time to time in accordance with this Clause 20.3), or shall be sent by prepaid first-class post, recorded delivery or by commercial courier, at its registered office (if a company) or (in any other case) its principal place of business, subject to the conditions set out in Clause 20.3.4 below.

- 20.3.2 Notices sent by email shall include the notice as a PDF email attachment and state in the subject line that the email contains a notice under the Contract.

- 20.3.3 Any notice or communication shall be deemed to have been duly received if sent by e-mail at 9.00 am on the next Business Day after transmission or, if sent by prepaid first-class post or recorded delivery, at 9.00 am on the second Business Day after posting, or if delivered by commercial courier, on the date and at the time that the courier's delivery receipt is signed.

- 20.3.4 Where notice is sent by sent by prepaid first-class post, recorded delivery or by commercial courier, at its registered office (if a company) or (in any other case) its principal place of

business, a copy of such notice shall also be sent by email in accordance with the requirements of Clause 20.3.1 and 20.3.2 above.

20.3.5 This Clause 20.3 shall not apply to the service of any proceedings or other documents in any legal action.

20.4 **Waiver and cumulative remedies:**

20.4.1 A waiver of any right under the Contract is only effective if it is in writing and shall not be deemed to be a waiver of any subsequent breach or default. No failure or delay by a party in exercising any right or remedy under the Contract or by law shall constitute a waiver of that or any other right or remedy, nor preclude or restrict its further exercise. No single or partial exercise of such right or remedy shall preclude or restrict the further exercise of that or any other right or remedy.

20.4.2 Unless specifically provided otherwise, rights arising under the Contract are cumulative and do not exclude rights provided by law.

20.5 **Severance:**

20.5.1 If a court or any other competent authority finds that any provision (or part of any provision) of the Contract is invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed deleted, and the validity and enforceability of the other provisions of the Contract shall not be affected.

20.5.2 If any invalid, unenforceable or illegal provision of the Contract would be valid, enforceable and legal if some part of it were deleted, the provision shall apply with the minimum modification necessary to make it legal, valid and enforceable.

20.6 **No partnership:** Nothing in the Contract is intended to, or shall be deemed to, constitute a partnership or joint venture of any kind between any of the parties, nor constitute a party the agent of the other party for any purpose. Neither party shall have authority to act as agent for, or to bind, the other party in any way. For the avoidance of doubt nothing in the Contract shall be deemed to make the Supplier an agent, employee or partner of LSE or FCDO.

20.7 **Third parties:** A person who is not a party to the Contract shall not have any rights under or in connection with it.

20.8 **Variation:** Any variation, including any additional terms and conditions, to the Contract shall only be binding when agreed in writing and signed by an Authorised Officer of LSE.

20.9 **Governing law:** The Contract shall be governed by and interpreted in accordance with the laws of England and Wales.

20.10 **Jurisdiction:**

20.10.1 If the Supplier is domiciled in the United Kingdom or European Union (in circumstances where court judgements made in the United Kingdom are recognised by other members of the European Union as being enforceable in their jurisdictions), the exclusive forum for settling any Disputes which may arise out of or in connection with the Contract shall be the courts of England and Wales.

20.10.2 If the Supplier is not domiciled in the United Kingdom or European Union (or is domiciled in the European Union but the United Kingdom has ceased to be a member of the European Union in circumstances where court judgments made in the United Kingdom are not

recognised by members of the European Union as being enforceable in their jurisdictions) any Dispute which may arise out of or in connection with the Contract shall be exclusively referred to and finally resolved by arbitration under the LCIA Rules to be held virtually by conference call, videoconference or using other communications technology with participants in one or more geographical places, unless both parties agree that an in-person hearing is appropriate given the nature of the dispute. Any remote arbitration proceedings shall utilise appropriate video conferencing software (or other options listed above) with sufficient security setup to protect the confidentiality of the arbitration. The LCIA Rules are deemed to be incorporated into this Clause by reference in respect of such Disputes. The number of arbitrators shall be one. The language to be used in the arbitral proceedings shall be English and the law of the seat of the arbitration shall apply. Any fees for the arbitration shall be divided equally between the parties.

20.11 **Entire agreement:** The Contract constitutes the entire agreement between the parties relating to the subject matter of the Contract. The Contract supersedes all previous correspondence, writings, facsimiles, e-mails and other electronic communications), and verbal communications between the Supplier and LSE regarding the Services, none of which shall form any part of the Contract save to the extent that they are expressly incorporated into the Contract. For the avoidance of doubt, nothing in the Contract shall exclude or limit liability for fraudulent misrepresentation.

Annex 3: Supplier Code of Conduct

Principles

LSE aims to create an inclusive culture of best practice with the Suppliers with whom it engages and which receive UK taxpayers' funds. All Suppliers should adhere to the overarching principles of the LSE Supplier Code of Conduct (hereafter "Code of Conduct").

Overarching Principles for Suppliers

- ✓ **Act responsibly and with integrity**
- ✓ **Be transparent and accountable**
- ✓ **Seek to improve value for money**
- ✓ **Demonstrate commitment to poverty reduction and FCDO priorities¹**
- ✓ **Demonstrate commitment to wider HMG priorities²**

Supplier responsibilities

Suppliers and their sub-contractors (referred to in the following as "delivery chain partners") should ensure they have read and understood this Code of Conduct and their required compliance level and seek clarification from LSE where necessary. In particular, it is important that Suppliers and their delivery chain partners understand any risks and have systems in place to manage them. The compliance levels are: -

Compliance Level 2 – Suppliers with an individual contract value below £1m, or two or more contracts with LSE with a value of less than £5m;

Compliance Level 3 - Suppliers with an individual Contract value, or component of a Contract, with a value below the EU contracting threshold found here: -

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/850566/PN_for_New_Thresholds_2020_pdf.pdf

At this level (3) Suppliers are required to adhere to the Overarching Principles for Suppliers as set out in the above table and recognise, mitigate and manage risks. These Suppliers will not be monitored against the contractual Key Performance Indicators (KPIs) as referenced in Annex 3a and 3b.

Scope

This Code of Conduct forms part of the LSE (IGC) Supplier Terms and Conditions and full compliance and annual verification via a signed declaration (if applicable), to be found at Annex 3b, is mandatory for contracted Suppliers. Adherence to the Code of Conduct at the appropriate level is also a requirement for LSE's direct Suppliers and their delivery chain partners in receipt of FCDO funding from LSE. LSE will monitor Suppliers in six priority areas as set out below using a set of Key Performance Indicators (KPIs) as referenced in Annex 3a and 3b.

¹ <https://www.gov.uk/government/organisations/department-for-international-development/about#priorities>

² <https://www.gov.uk/government/organisations/hm-treasury/about#priorities>

1. Value for Money and Governance

Key Performance Indicators KPI 1 a - b

Value for Money and financial transparency is an essential requirement of all LSE commissioned work. All Suppliers must seek to maximise development results, whilst driving cost efficiency, throughout the life of commissioned programmes. This includes budgeting and pricing realistically and appropriately to reflect delivery requirements and levels of risk over the life of the programme. It also includes managing uncertainty and change to protect value in the often challenging environments that we work in.

Suppliers must demonstrate that they are pursuing continuous improvement and applying stringent financial management and governance to reduce waste and improve efficiency in their internal operations and within the delivery chain. LSE expects Suppliers to demonstrate openness and honesty and to be realistic about capacity and capability at all times, accepting accountability and responsibility for performance along the full delivery chain, in both every-day and exceptional circumstances.

Specific requirements include:

- ✓ A transparent, open book approach, which enables scrutiny of value for money;
- ✓ Strict adherence to all UK (if applicable) and in-country government tax requirements;
- ✓ Processes for timely identification and resolution of issues which might be requested by LSE at any time.

2. Ethical Behaviour

Key Performance Indicators KPI 2 a- f

LSE Suppliers and their delivery chain partners act on behalf of the UK government and interact globally with country governments, other aid donors and their delivery partners, many stakeholders including citizens and directly and indirectly with aid beneficiaries. These interactions must therefore meet the highest standards of ethical and professional behaviour in order to uphold the reputation of the UK government.

Arrangements and relationships entered into, whether with or on behalf of LSE, must be free from bias, conflict of interest or the undue influence of others. Particular care must be taken by Suppliers and delivery chain staff who:

- a) are directly involved in the management of a programme or procurement of services; or
- b) who engage with i) frontline FCDO staff ii) other deliverers of aid iii) beneficiaries (of aid)

Where those in a) and b) could be susceptible to undue negative or detrimental influence.

Suppliers and their delivery chain partners must declare to LSE where there may be instances or allegations of previous unethical behaviour by an existing or potential staff member or where there is a known or suspected conflict of interest. Where a potential or existing staff member has been employed by FCDO or the Crown in the preceding two years Suppliers and their delivery chain partner must provide proof of compliance with the HMG approval requirements under the Business Appointment Rules.

Suppliers and their delivery chain partners must have the following policies and procedures in place:

- ✓ Development and proof of application and embedding of a Staff Recruitment, Management and Retention policy (which must address circumstances where there may be potential or actual conflict of interest and embedding of a Whistleblowing Policy)

- ✓ Ongoing monitoring of potential or existing personal, business or professional conflict of interest and their mitigation and management
- ✓ Ethical training for every staff member and staff updates in ethical working practices suitable to the development sector (e.g. UN Global Compact principles) including awareness of modern day slavery and human rights abuses
- ✓ Procedures setting out how, staff involved in FCDO funded business, can immediately report all suspicions or allegations of aid diversion, fraud, money laundering or counter terrorism finance to the FCDO Counter Fraud and Whistleblowing Unit (CFWU) at reportingconcerns@FCDO.gov.uk or on +44(0)1355 843747.

3. Transparency and Delivery Chain Management

Key Performance Indicators KPI 3 a – b

LSE requires full delivery chain transparency from all Suppliers. All direct Suppliers and their delivery chain partners must adhere to wider HMG policy initiatives including the support and capacity building of micro, small and medium sized enterprises (MSMEs), prompt payment, adherence to human rights and modern slavery policies and support for economic growth in developing countries.

LSE recognises the critical value that downstream delivery partners contribute. Direct Suppliers must engage their delivery chain partners in a manner that is consistent with LSE’s treatment of its Suppliers. This includes, but is not limited to: appropriate pricing of services; fiduciary and financial risk management processes; applying transparent and responsive measures where delivery chain partners underperform against the KPI areas; taking a zero tolerance approach to tax evasion, corruption, bribery and fraud in subsequent service delivery or in partnership agreements. Direct Suppliers must cascade the principles of the Code of Conduct throughout their delivery chain to ensure LSE ethical behaviour standards are embedded and maintained.

Specific requirements for direct Suppliers include:

- ✓ Provide assurance to LSE that the policies and practices of their delivery chain partners and affiliates comply with the Code of Conduct;
- ✓ Ensuring delivery chain partner employees are expressly notified of the FCDO ‘reporting concerns’ mail box³ found on FCDO’s external website and of the circumstances in which this should be used;

4. Environmental issues

LSE Suppliers must be committed to high environmental standards, recognising that FCDO’s activities may change the way people use and rely on the environment, or may affect or be affected by environmental conditions.

³ <https://www.gov.uk/government/organisations/department-for-international-development/about#reporting-fraud>

5. Terrorism and Security

Key Performance Indicators KPI 5 a – c

LSE Suppliers must implement due diligence processes to provide assurance that UK Government funding is not used in any way that contravenes the provisions of the Terrorism Act 2000, and any subsequent regulations pursuant to this Act.

LSE Suppliers must maintain high levels of data security in accordance with the Data Protection Act 1998 and any subsequent regulations pursuant to this Act, or new Act and with the General Data Protection Regulation (Directive 95/46/EC).

Specific requirements:

- ✓ Development and proof of application and embedding of a comprehensive Terrorism and Security Policy
- ✓ Development and proof of application and embedding of personal data processing processes within a Data Protection Policy
- ✓ LSE Suppliers must safeguard the integrity and security of their IT and mobile communications systems in line with the HMG Cyber Essentials Scheme⁴. Award of the Cyber Essentials or Cyber Essential Plus badges would provide organisational evidence of meeting the UK Government-endorsed standard;
- ✓ All LSE Suppliers who manage aid programmes with a digital element must adhere to the global Principles for Digital Development⁵, which sets out best practice in technology-enabled programmes
- ✓ Ensure that FCDO funding is not linked to terrorist offences, terrorist activities or financing.

6. Safeguarding, Social Responsibility and Human Rights

Key Performance Indicators: KPI 6 a – b

Safeguarding, social responsibility and respect for human rights are central to LSE's expectations of its Suppliers. Suppliers must ensure that robust procedures are adopted and maintained to eliminate the risk of poor human rights practices within complex delivery chain environments funded by FCDO and LSE. These practices include sexual exploitation, abuse and harassment; all forms of child abuse and inequality or discrimination on the basis of race, gender, age, religion, sexuality, culture or disability. Suppliers must place an emphasis on the control of these and further unethical and illegal employment practices, such as modern day slavery, forced and child labour and other forms of exploitative and unethical treatment of workers and aid recipients. FCDO will expect a particular emphasis on the management of these issues in high risk fragile and conflict affected states (FCAS), with a focus on ensuring remedy and redress if things go wrong.

Specific requirements:

- ✓ Development and application and embedding of a Safeguarding Policy;
- ✓ Delivery of Social Responsibility, Human Rights and Safeguarding training throughout the delivery chain;

⁴ <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview>

⁵ <https://digitalprinciples.org>

⁶ http://ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C138

⁷ <https://www.ethicaltrade.org.eti-base-code>

- ✓ Practices in line with the International Labour Organisation (ILO) 138⁶ and the Ethical Trading Initiative (ETI) Base Code⁷ are to be encouraged throughout the delivery chain;
- ✓ Policies to embed good practice in line with the UN Global Compact Guiding Principles 1 & 2 on business and human rights throughout the delivery chain are required, as detailed in Annex 2;
- ✓ Overarching consideration given to building local capacity and promoting the involvement of people whose lives are affected by business decisions.

Annex 3a

Compliance KPIs and contractual checking mechanisms - LSE Contracts

Maintaining standards of assurance and driving sustainable improvements, in connection with the Code of Conduct’s principles through Supplier relationships is a key focus for LSE.

Suppliers and their delivery chain compliance checking processes will take place in accordance with the agreed compliance levels and the specific contractual clauses down the delivery chain, LSE may undertake compliance checks.

Where appropriate, a plan setting out the Code of Conduct delivery methodology for the Supplier arrangements during the contract term may be jointly developed with LSE during Contract mobilisation.

Contract Checks and Compliance KPIs	KPI target	Specific Contractual link or other relevant document (where applicable)	Checking mechanism	
i.	Declaration of acceptance of the LSE Supplier Code of Conduct	Annual declaration submitted by contracted Supplier on behalf of delivery chain	Supplier T&Cs Clause 3.3. and Clause 20.2.2 b	Declaration of acceptance at the applicable level of compliance with each of the 6 sections received
1.	<u>VfM and Governance standards</u>			
a)	VfM being maximised over the life of a contract 1. By confirmation of annual profit level fluctuations since proposal submittal 2. by timely identification and resolution of issues	Updated documentation submitted once annually Updated documentation submitted once annually	Supplier T&Cs Clause 12	Compliance checks Annual contract review/programme management Compliance checks
b)	<u>Tax Declaration (HMRC format)</u> <ul style="list-style-type: none"> • Tax the organisation paid on profits made in the last 3 years, and in which countries • Compliance with relevant country level tax regulations fully understood and met 	Annually updated documentation submitted by contracted supplier and on behalf of delivery chain partners	Supplier T&Cs Clauses 12, 3.8	Annual return Compliance checks

2.	<u>Ethical Behaviour</u>			
a)	Recruitment policy (which must address circumstances where there may be potential or actual conflict of interest)	Updated policy documentation submitted once annually by contracted supplier and on behalf of delivery chain partners	Supplier T&Cs Clauses 10 & 3.4	Annual return Compliance checks
b)	Ongoing conflict of interest, mitigation and management	As 2a. above	Supplier T&Cs Clause 3.4	Annual return Compliance checks
c)	Refresher ethical training and staff updates (including disclosure restrictions on FCDO confidential information)	Copy of training logs provided. Delivery in accordance with training programme in place	Supplier T&Cs Clause, 14, 10 & 3.4	Annual return Compliance checks
d)	A workforce whistleblowing policy	Continuous workforce awareness maintained Policy in place	Supplier T&Cs Clause 19	Annual return Compliance checks
e)	<p>1. Procedures setting out how, staff involved in FCDO funded business, can immediately report all suspicions or allegations of aid diversion, fraud, money laundering or counter terrorism finance to the Counter Fraud and Whistleblowing Unit (CFWU) at reportingconcerns@FCDO.gov.uk or on +44(0)1355 843747</p> <p>2. Employees working on FCDO Contracts fully aware of the FCDO external website reporting concerns mailbox</p>	<p>Continuous awareness maintained</p> <p>Procedure in place</p> <p>Continuous awareness maintained</p>	<p>Supplier T&Cs 19 & 3.4</p> <p>Supplier T&Cs Clause 19</p>	<p>Annual return Compliance checks</p> <p>Annual return Compliance checks</p>
f)	<p>Declarations of direct or sub-contractor staff members proposed to work on FCDO funded business if employed by FCDO or the Crown in the preceding two years</p> <p>Suppliers and their delivery chain partners must provide proof of compliance with the HMG approval requirements under the business appointment rules</p>	Details submitted as applicable	<p>Supplier T&Cs Clause 19</p> <p>HMG business appointment rules</p>	<p>Annual return Compliance checks</p> <p>Contract management</p>
3.	<u>Transparency and Delivery Chain Management</u>			
a)	Tax evasion, bribery, corruption and fraud - statements of assurance provided	Updated documentation submitted once annually	Supplier T&Cs 3.8	Periodic and annual return spot checks. Compliance checks
b)	All delivery chain partner employees working on FCDO Contracts fully aware of the FCDO reporting concerns mailbox	Updated documentation submitted once annually	Supplier T&Cs Clause 19	Periodic and annual return spot checks

	reportingconcerns@FCDO.gov.uk			
5.	<u>Terrorism and Security</u>			
a)	Up to date status declaration regarding the reporting of terrorist offences or offences linked to terrorist activities or financing	Updated documentation submitted if and when changes identified since initial Contractual Annual Compliance Declaration	Contractual Annual Compliance Declaration	Annual return spot checks Compliance checks
b)	Certification at or above the level set out in the initial Contractual Annual Compliance Declaration	Updated documentation submitted if changes identified since initial Contractual Annual Compliance Declaration	Contractual Annual Compliance Declaration	Annual return Compliance checks
c)	Data managed in accordance with FCDO Security Policy and systems in accordance with the HMG Cyber Essentials Scheme	Updated documentation submitted if changes identified since / initial Contractual Annual Compliance Declaration	Supplier T&Cs Clause 15.14.5& 8	Compliance checks
6.	<u>Safeguarding, Social Responsibility and Human Rights</u>			
a)	Agreed level of measures in place and cascaded to assure the prevention of actual, attempted or threatened sexual exploitation or abuse or other forms of inequality or discrimination by employees or any other persons engaged and controlled by the Supply Partner to perform any activities relating to FCDO funded work. Robust procedures for the reporting of suspected misconduct, illegal acts or failures to investigate in place	Updated documentation submitted once annually	Supplier T&Cs Clause 19	Due Diligence Assessment Compliance checks
b)	Number and details of any organisational safeguarding allegations reported	Updated documentation submitted if and when changes identified since initial Contractual Annual Compliance Declaration		Annual checks Compliance checks

Contractual Annual Compliance Declaration**(Compliance Level 2 Suppliers)**

Prior to Contract Award and thereafter on an annual basis on the anniversary of the Contract Award, the Supplier is required to submit a Compliance Declaration in connection with the management of any LSE Contract in place and on behalf of their delivery chain partners. Suppliers should be aware that spot check compliance monitoring may take place to verify responses.

KPI Compliance Area		Commentary	CEO Signatory Name	Signature & date of signing
1.	<u>VfM and Governance standards</u>			
a)	VfM maximisation over contract life 1. Annual confirmation of % profit on contract 2. timely identification and resolution of issues			
b)	<u>Tax Declaration (HMRC format)</u> Comply with all tax requirements			
2.	<u>Ethical Behaviour</u>			
a)	Adherence to agreed conflict of interest management procedures			
b)	Evidence of workforce ethical training updates taking place			
c)	Confirmation of direct and delivery chain partner compliance with the HMG approval requirements under the Business Appointment Rules.			
d)	Confirmation and full evidence of awareness of an up to date workforce whistleblowing policy			
e)	Procedures in place and full evidence of awareness of how, staff involved in FCDO funded business, can immediately report all suspicions or allegations of aid diversion, fraud, money laundering or counter terrorism finance to the Counter Fraud and Whistleblowing Unit (CFWU) at reportingconcerns@FCDO.gov.uk or on +44(0)1355 843747			
f)	HMG Business appointment rules followed - Conflict of Interest (COI) declarations made for direct or delivery chain staff members proposed to work on FCDO funded business if employed by FCDO or the Crown in the preceding two years.			
3.	<u>Transparency and Delivery Chain Management</u>			
a)	Assurance there has been no change to previous statements provided in relation to tax evasion,			

	bribery, corruption and fraud			
b)	Confirmation that all delivery chain partners' employees working on FCDO Contracts are fully aware of the FCDO reporting concerns mailbox reportingconcerns@FCDO.gov.uk			
5.	<u>Terrorism and Security</u>			
a)	Up to date status declaration regarding the reporting of terrorist offences or offences linked to terrorist activities or financing			
b)	No engaged employees or delivery chain partner personnel appears on the Home Office Prescribed Terrorist Organisations List			
c)	Data is managed in accordance with FCDO security policy and systems are in accordance with the HMG cyber essentials scheme			
6.	<u>Safeguarding, Social Responsibility and Human Rights</u>			
a)	1.To prevent actual, attempted or threatened sexual exploitation and abuse or other forms of inequality or discrimination by employees or any other persons engaged and controlled by the Supply Partner to perform any activities relating to FCDO funded work 2.For reporting suspected misconduct, illegal acts or failures to investigate actual attempted or threatened sexual exploitation or abuse			
b)	Numbers and details of organisational safeguarding allegations reported			

ANNEX 4 (a)

Transfers of Personal Data to non-EEA Countries

The Parties will comply with the provisions of the Standard Data Protection Clauses issued by the Commissioner under S119A(1) Data Protection Act 2018, International Data Transfer Agreement, version A1.0, in force 21 March 2022 ("IDTA") and signature of this Contract by the Parties shall be deemed to include signature of the IDTA.

Link to IDTA:

[international-data-transfer-agreement.pdf \(ico.org.uk\)](#) , also attached as Annex 4 (b).

The following details shall apply to the IDTA:

(a) Table 1: Parties and signatures

Start date	The Commencement Date of the Contract	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	<p>Full legal name: London School of Economics and Political Science</p> <p>Main address (if a company registered address): Houghton Street London WC2A 2AE</p> <p>Official registration number (if any) (company number or similar identifier): 70527</p>	The Supplier, as defined in the Appointment Letter
Key Contact	<p>Full Name (optional): Rachael Maguire</p> <p>Job Title: Data Protection Officer</p> <p>Contact details including email: r.e.maguire@lse.ac.uk</p>	The Supplier signatory

Table 2: Transfer Details

UK country's law that governs the IDTA:	<input checked="" type="checkbox"/> England and Wales <input type="checkbox"/> Northern Ireland <input type="checkbox"/> Scotland
Primary place for legal claims to be made by the Parties	<input checked="" type="checkbox"/> England and Wales <input type="checkbox"/> Northern Ireland

	<input type="checkbox"/> Scotland
The status of the Exporter	<p>In relation to the Processing of the Transferred Data:</p> <input checked="" type="checkbox"/> Exporter is a Controller <input type="checkbox"/> Exporter is a Processor or Sub-Processor
The status of the Importer	<p>In relation to the Processing of the Transferred Data:</p> <input checked="" type="checkbox"/> Importer is a Controller <input type="checkbox"/> Importer is the Exporter's Processor or Sub-Processor <input type="checkbox"/> Importer is not the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)
Whether UK GDPR applies to the Importer	<input type="checkbox"/> UK GDPR applies to the Importer's Processing of the Transferred Data <input checked="" type="checkbox"/> UK GDPR does not apply to the Importer's Processing of the Transferred Data
Linked Agreement	Not applicable
Term	<p>The Importer may Process the Transferred Data for the following time period:</p> <input type="checkbox"/> the period for which the Linked Agreement is in force <input type="checkbox"/> time period: <input checked="" type="checkbox"/> (only if the Importer is a Controller or not the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose.
Ending the IDTA before the end of the Term	<input checked="" type="checkbox"/> the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing. <input type="checkbox"/> the Parties can end the IDTA before the end of the Term by serving: <input type="checkbox"/> months' written notice, as set out in Section Error! Reference source not found. (How to end this IDTA without there being a breach).

<p>Ending the IDTA when the Approved IDTA changes</p>	<p>Which Parties may end the IDTA as set out in Section Error! Reference source not found.:</p> <p><input type="checkbox"/> Importer</p> <p><input checked="" type="checkbox"/> Exporter</p> <p><input type="checkbox"/> neither Party</p>
<p>Can the Importer make further transfers of the Transferred Data?</p>	<p><input checked="" type="checkbox"/> The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section Error! Reference source not found. (Transferring on the Transferred Data).</p> <p><input type="checkbox"/> The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section Error! Reference source not found. (Transferring on the Transferred Data).</p>
<p>Specific restrictions when the Importer may transfer on the Transferred Data</p>	<p>The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1:</p> <p><input checked="" type="checkbox"/> if the Exporter tells it in writing that it may do so.</p> <p><input type="checkbox"/> to: [REDACTED]</p> <p><input type="checkbox"/> to the authorised receivers (or the categories of authorised receivers) set out in:</p> <p><input type="checkbox"/> there are no specific restrictions.</p>
<p>Review Dates</p>	<p><input checked="" type="checkbox"/> No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data</p> <p>First review date: [REDACTED]</p> <p>The Parties must review the Security Requirements at least once:</p> <p><input type="checkbox"/> each [REDACTED] month(s)</p> <p><input type="checkbox"/> each quarter</p> <p><input type="checkbox"/> each 6 months</p> <p><input type="checkbox"/> each year</p> <p><input type="checkbox"/> each [REDACTED] year(s)</p>

- each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment

Table 3: Transferred Data

Transferred Data	<p>The personal data to be sent to the Importer under this IDTA consists of:</p> <p>Publicly Disclosed Data</p>
Special Categories of Personal Data and criminal convictions and offences	<p>The Transferred Data includes data relating to:</p> <ul style="list-style-type: none"> <input type="checkbox"/> racial or ethnic origin <input type="checkbox"/> political opinions <input type="checkbox"/> religious or philosophical beliefs <input type="checkbox"/> trade union membership <input type="checkbox"/> genetic data <input type="checkbox"/> biometric data for the purpose of uniquely identifying a natural person <input type="checkbox"/> physical or mental health <input type="checkbox"/> sex life or sexual orientation <input type="checkbox"/> criminal convictions and offences <input checked="" type="checkbox"/> none of the above <input type="checkbox"/> set out in:
Relevant Subjects	<p>The Data Subjects of the Transferred Data are:</p> <p>LSE Employees</p>
Purpose	<ul style="list-style-type: none"> <input type="checkbox"/> The Importer may Process the Transferred Data for the following purposes: the legitimate interests pursued by the controller or by a third party.

Table 4 - Security Requirements

Security	of Please see attached Annex 4c
-----------------	--

Transmission	
Security of Storage	Please see attached Annex 4c
Security Processing of	Please see attached Annex 4c
Organisational security measures	Please see attached Annex 4c
Technical security minimum requirements	Please see attached Annex 4c
Updates to the Security Requirements	<input type="checkbox"/> The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to. <input checked="" type="checkbox"/> The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Part 2: Extra Protection Clauses - Not applicable

Part 3: Commercial Clauses - Not applicable.



Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Agreement

VERSION A1.0, in force 21 March 2022

This IDTA has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties and signatures

Start date		
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: <input type="text"/> Trading name (if different): <input type="text"/> Main address (if a company registered address): <input type="text"/> Official registration number (if any) (company number or similar identifier): <input type="text"/>	Full legal name: <input type="text"/> Trading name (if different): <input type="text"/> Main address (if a company registered address): <input type="text"/> Official registration number (if any) (company number or similar identifier): <input type="text"/>
Key Contact	Full Name (optional): <input type="text"/> Job Title: <input type="text"/>	Full Name (optional): <input type="text"/> Job Title: <input type="text"/>

	Contact details including email: [REDACTED]	Contact details including email: [REDACTED]
Importer Data Subject Contact		Job Title: [REDACTED] Contact details including email: [REDACTED]
Signatures confirming each Party agrees to be bound by this IDTA	Signed for and on behalf of the Exporter set out above Signed: [REDACTED] Date of signature: [REDACTED] Full name: [REDACTED] Job title: [REDACTED]	Signed for and on behalf of the Importer set out above Signed: [REDACTED] Date of signature: [REDACTED] Full name: [REDACTED] Job title: [REDACTED]

Table 2: Transfer Details

UK country's law that governs the IDTA:	<input type="checkbox"/> England and Wales <input type="checkbox"/> Northern Ireland <input type="checkbox"/> Scotland
Primary place for legal claims to be made by the Parties	<input type="checkbox"/> England and Wales <input type="checkbox"/> Northern Ireland <input type="checkbox"/> Scotland
The status of the Exporter	In relation to the Processing of the Transferred Data: <input type="checkbox"/> Exporter is a Controller <input type="checkbox"/> Exporter is a Processor or Sub-Processor
The status of the Importer	In relation to the Processing of the Transferred Data: <input type="checkbox"/> Importer is a Controller <input type="checkbox"/> Importer is the Exporter's Processor or Sub-Processor <input type="checkbox"/> Importer is not the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)

<p>Whether UK GDPR applies to the Importer</p>	<p><input type="checkbox"/> UK GDPR applies to the Importer’s Processing of the Transferred Data</p> <p><input type="checkbox"/> UK GDPR does not apply to the Importer’s Processing of the Transferred Data</p>
<p>Linked Agreement</p>	<p>If the Importer is the Exporter’s Processor or Sub-Processor – the agreement(s) between the Parties which sets out the Processor’s or Sub-Processor’s instructions for Processing the Transferred Data:</p> <p>Name of agreement: [REDACTED]</p> <p>Date of agreement: [REDACTED]</p> <p>Parties to the agreement: [REDACTED]</p> <p>Reference (if any): [REDACTED]</p> <p>Other agreements – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement:</p> <p>Name of agreement: [REDACTED]</p> <p>Date of agreement: [REDACTED]</p> <p>Parties to the agreement: [REDACTED]</p> <p>Reference (if any): [REDACTED]</p> <p>If the Exporter is a Processor or Sub-Processor – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter’s instructions for Processing the Transferred Data:</p> <p>Name of agreement: [REDACTED]</p> <p>Date of agreement: [REDACTED]</p> <p>Parties to the agreement: [REDACTED]</p> <p>Reference (if any): [REDACTED]</p>
<p>Term</p>	<p>The Importer may Process the Transferred Data for the following time period:</p> <p><input type="checkbox"/> the period for which the Linked Agreement is in force</p> <p><input type="checkbox"/> time period:</p>

	<p><input type="checkbox"/> (only if the Importer is a Controller or not the Exporter’s Processor or Sub-Processor) no longer than is necessary for the Purpose.</p>
<p>Ending the IDTA before the end of the Term</p>	<p><input type="checkbox"/> the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing.</p> <p><input type="checkbox"/> the Parties can end the IDTA before the end of the Term by serving:</p> <p> [] months’ written notice, as set out in Section 29 (How to end this IDTA without there being a breach).</p>
<p>Ending the IDTA when the Approved IDTA changes</p>	<p>Which Parties may end the IDTA as set out in Section 29.2:</p> <p><input type="checkbox"/> Importer</p> <p><input type="checkbox"/> Exporter</p> <p><input type="checkbox"/> neither Party</p>
<p>Can the Importer make further transfers of the Transferred Data?</p>	<p><input type="checkbox"/> The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).</p> <p><input type="checkbox"/> The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).</p>
<p>Specific restrictions when the Importer may transfer on the Transferred Data</p>	<p>The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1:</p> <p><input type="checkbox"/> if the Exporter tells it in writing that it may do so.</p> <p><input type="checkbox"/> to: []</p> <p><input type="checkbox"/> to the authorised receivers (or the categories of authorised receivers) set out in:</p> <p><input type="checkbox"/> there are no specific restrictions.</p>
<p>Review Dates</p>	<p><input type="checkbox"/> No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data</p> <p>First review date: []</p>

	<p>The Parties must review the Security Requirements at least once:</p> <ul style="list-style-type: none"> <input type="checkbox"/> each [] month(s) <input type="checkbox"/> each quarter <input type="checkbox"/> each 6 months <input type="checkbox"/> each year <input type="checkbox"/> each [] year(s) <input type="checkbox"/> each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment
--	--

Table 3: Transferred Data

Transferred Data	<p>The personal data to be sent to the Importer under this IDTA consists of:</p> <ul style="list-style-type: none"> <input type="checkbox"/> The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The categories of Transferred Data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Special Categories of Personal Data and criminal convictions and offences	<p>The Transferred Data includes data relating to:</p> <ul style="list-style-type: none"> <input type="checkbox"/> racial or ethnic origin <input type="checkbox"/> political opinions <input type="checkbox"/> religious or philosophical beliefs <input type="checkbox"/> trade union membership <input type="checkbox"/> genetic data <input type="checkbox"/> biometric data for the purpose of uniquely identifying a natural person <input type="checkbox"/> physical or mental health <input type="checkbox"/> sex life or sexual orientation <input type="checkbox"/> criminal convictions and offences <input type="checkbox"/> none of the above <input type="checkbox"/> set out in:

	<p>And:</p> <ul style="list-style-type: none"> <input type="checkbox"/> The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The categories of special category and criminal records data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
<p>Relevant Data Subjects</p>	<p>The Data Subjects of the Transferred Data are:</p> <ul style="list-style-type: none"> <input type="checkbox"/> The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The categories of Data Subjects will not update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
<p>Purpose</p>	<ul style="list-style-type: none"> <input type="checkbox"/> The Importer may Process the Transferred Data for the following purposes: <input type="checkbox"/> The Importer may Process the Transferred Data for the purposes set out in: <p>In both cases, any other purposes which are compatible with the purposes set out above.</p> <ul style="list-style-type: none"> <input type="checkbox"/> The purposes will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Table 4: Security Requirements

<p>Security of Transmission</p>	
--	--

Security of Storage	
Security of Processing	
Organisational security measures	
Technical security minimum requirements	
Updates to the Security Requirements	<p><input type="checkbox"/> The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to.</p> <p><input type="checkbox"/> The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.</p>

Part 2: Extra Protection Clauses

Extra Protection Clauses:	
(i) Extra technical security protections	
(ii) Extra organisational protections	

(iii) Extra contractual protections

Part 3: Commercial Clauses

Commercial Clauses

Part 4: Mandatory Clauses

Information that helps you to understand this IDTA

1. This IDTA and Linked Agreements

- 1.1 Each Party agrees to be bound by the terms and conditions set out in the IDTA, in exchange for the other Party also agreeing to be bound by the IDTA.
- 1.2 This IDTA is made up of:
 - 1.2.1 Part one: Tables;
 - 1.2.2 Part two: Extra Protection Clauses;
 - 1.2.3 Part three: Commercial Clauses; and
 - 1.2.4 Part four: Mandatory Clauses.
- 1.3 The IDTA starts on the Start Date and ends as set out in Sections 29 or 30.
- 1.4 If the Importer is a Processor or Sub-Processor instructed by the Exporter: the Exporter must ensure that, on or before the Start Date and during the Term, there is a Linked Agreement which is enforceable between the Parties and which complies with Article 28 UK GDPR (and which they will ensure continues to comply with Article 28 UK GDPR).
- 1.5 References to the Linked Agreement or to the Commercial Clauses are to that Linked Agreement or to those Commercial Clauses only in so far as they are consistent with the Mandatory Clauses.

2. Legal Meaning of Words

- 2.1 If a word starts with a capital letter it has the specific meaning set out in the Legal Glossary in Section 36.
- 2.2 To make it easier to read and understand, this IDTA contains headings and guidance notes. Those are not part of the binding contract which forms the IDTA.

3. You have provided all the information required

- 3.1 The Parties must ensure that the information contained in Part one: Tables is correct and complete at the Start Date and during the Term.
- 3.2 In Table 2: Transfer Details, if the selection that the Parties are Controllers, Processors or Sub-Processors is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws) then:
 - 3.2.1 the terms and conditions of the Approved IDTA which apply to the correct option which was not selected will apply; and
 - 3.2.2 the Parties and any Relevant Data Subjects are entitled to enforce the terms and conditions of the Approved IDTA which apply to that correct option.
- 3.3 In Table 2: Transfer Details, if the selection that the UK GDPR applies is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws), then the terms and conditions of the IDTA will still apply to the greatest extent possible.

4. How to sign the IDTA

- 4.1 The Parties may choose to each sign (or execute):
 - 4.1.1 the same copy of this IDTA;
 - 4.1.2 two copies of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement;
 - 4.1.3 a separate, identical copy of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement,

unless signing (or executing) in this way would mean that the IDTA would not be binding on the Parties under Local Laws.

5. Changing this IDTA

- 5.1 Each Party must not change the Mandatory Clauses as set out in the Approved IDTA, except only:

- 5.1.1 to ensure correct cross-referencing: cross-references to Part one: Tables (or any Table), Part two: Extra Protections, and/or Part three: Commercial Clauses can be changed where the Parties have set out the information in a different format, so that the cross-reference is to the correct location of the same information, or where clauses have been removed as they do not apply, as set out below;
- 5.1.2 to remove those Sections which are expressly stated not to apply to the selections made by the Parties in Table 2: Transfer Details, that the Parties are Controllers, Processors or Sub-Processors and/or that the Importer is subject to, or not subject to, the UK GDPR. The Exporter and Importer understand and acknowledge that any removed Sections may still apply and form a part of this IDTA if they have been removed incorrectly, including because the wrong selection is made in Table 2: Transfer Details;
- 5.1.3 so the IDTA operates as a multi-party agreement if there are more than two Parties to the IDTA. This may include nominating a lead Party or lead Parties which can make decisions on behalf of some or all of the other Parties which relate to this IDTA (including reviewing Table 4: Security Requirements and Part two: Extra Protection Clauses, and making updates to Part one: Tables (or any Table), Part two: Extra Protection Clauses, and/or Part three: Commercial Clauses); and/or
- 5.1.4 to update the IDTA to set out in writing any changes made to the Approved IDTA under Section 5.4, if the Parties want to. The changes will apply automatically without updating them as described in Section 5.4;

provided that the changes do not reduce the Appropriate Safeguards.

- 5.2 If the Parties wish to change the format of the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of the Approved IDTA, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- 5.3 If the Parties wish to change the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of this IDTA (or the equivalent information), they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- 5.4 From time to time, the ICO may publish a revised Approved IDTA which:

5.4.1 makes reasonable and proportionate changes to the Approved IDTA, including correcting errors in the Approved IDTA; and/or

5.4.2 reflects changes to UK Data Protection Laws.

The revised Approved IDTA will specify the start date from which the changes to the Approved IDTA are effective and whether an additional Review Date is required as a result of the changes. This IDTA is automatically amended as set out in the revised Approved IDTA from the start date specified.

6. Understanding this IDTA

6.1 This IDTA must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

6.2 If there is any inconsistency or conflict between UK Data Protection Laws and this IDTA, the UK Data Protection Laws apply.

6.3 If the meaning of the IDTA is unclear or there is more than one meaning, the meaning which most closely aligns with the UK Data Protection Laws applies.

6.4 Nothing in the IDTA (including the Commercial Clauses or the Linked Agreement) limits or excludes either Party's liability to Relevant Data Subjects or to the ICO under this IDTA or under UK Data Protection Laws.

6.5 If any wording in Parts one, two or three contradicts the Mandatory Clauses, and/or seeks to limit or exclude any liability to Relevant Data Subjects or to the ICO, then that wording will not apply.

6.6 The Parties may include provisions in the Linked Agreement which provide the Parties with enhanced rights otherwise covered by this IDTA. These enhanced rights may be subject to commercial terms, including payment, under the Linked Agreement, but this will not affect the rights granted under this IDTA.

6.7 If there is any inconsistency or conflict between this IDTA and a Linked Agreement or any other agreement, this IDTA overrides that Linked Agreement or any other agreements, even if those agreements have been negotiated by the Parties. The exceptions to this are where (and in so far as):

6.7.1 the inconsistent or conflicting terms of the Linked Agreement or other agreement provide greater protection for the Relevant Data Subject's rights, in which case those terms will override the IDTA; and

- 6.7.2 a Party acts as Processor and the inconsistent or conflicting terms of the Linked Agreement are obligations on that Party expressly required by Article 28 UK GDPR, in which case those terms will override the inconsistent or conflicting terms of the IDTA in relation to Processing by that Party as Processor.
- 6.8 The words “include”, “includes”, “including”, “in particular” are used to set out examples and not to set out a finite list.
- 6.9 References to:
- 6.9.1 singular or plural words or people, also includes the plural or singular of those words or people;
- 6.9.2 legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this IDTA has been signed; and
- 6.9.3 any obligation not to do something, includes an obligation not to allow or cause that thing to be done by anyone else.

7. Which laws apply to this IDTA

- 7.1 This IDTA is governed by the laws of the UK country set out in Table 2: Transfer Details. If no selection has been made, it is the laws of England and Wales. This does not apply to Section 35 which is always governed by the laws of England and Wales.

How this IDTA provides Appropriate Safeguards

8. The Appropriate Safeguards

- 8.1 The purpose of this IDTA is to ensure that the Transferred Data has Appropriate Safeguards when Processed by the Importer during the Term. This standard is met when and for so long as:
- 8.1.1 both Parties comply with the IDTA, including the Security Requirements and any Extra Protection Clauses; and
- 8.1.2 the Security Requirements and any Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach, including considering any Special Category Data within the Transferred Data.
- 8.2 The Exporter must:

- 8.2.1 ensure and demonstrate that this IDTA (including any Security Requirements and Extra Protection Clauses) provides Appropriate Safeguards; and
 - 8.2.2 (if the Importer reasonably requests) provide it with a copy of any TRA.
- 8.3 The Importer must:
- 8.3.1 before receiving any Transferred Data, provide the Exporter with all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including any information which may reasonably be required for the Exporter to carry out any TRA (the "Importer Information");
 - 8.3.2 co-operate with the Exporter to ensure compliance with the Exporter's obligations under the UK Data Protection Laws;
 - 8.3.3 review whether any Importer Information has changed, and whether any Local Laws contradict its obligations in this IDTA and take reasonable steps to verify this, on a regular basis. These reviews must be at least as frequent as the Review Dates; and
 - 8.3.4 inform the Exporter as soon as it becomes aware of any Importer Information changing, and/or any Local Laws which may prevent or limit the Importer complying with its obligations in this IDTA. This information then forms part of the Importer Information.
- 8.4 The Importer must ensure that at the Start Date and during the Term:
- 8.4.1 the Importer Information is accurate;
 - 8.4.2 it has taken reasonable steps to verify whether there are any Local Laws which contradict its obligations in this IDTA or any additional information regarding Local Laws which may be relevant to this IDTA.
- 8.5 Each Party must ensure that the Security Requirements and Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

9. Reviews to ensure the Appropriate Safeguards continue

- 9.1 Each Party must:
- 9.1.1 review this IDTA (including the Security Requirements and Extra Protection Clauses and the Importer Information) at regular intervals, to ensure that the IDTA remains accurate and up to date

and continues to provide the Appropriate Safeguards. Each Party will carry out these reviews as frequently as the relevant Review Dates or sooner; and

- 9.1.2 inform the other party in writing as soon as it becomes aware if any information contained in either this IDTA, any TRA or Importer Information is no longer accurate and up to date.
- 9.2 If, at any time, the IDTA no longer provides Appropriate Safeguards the Parties must Without Undue Delay:
 - 9.2.1 pause transfers and Processing of Transferred Data whilst a change to the Tables is agreed. The Importer may retain a copy of the Transferred Data during this pause, in which case the Importer must carry out any Processing required to maintain, so far as possible, the measures it was taking to achieve the Appropriate Safeguards prior to the time the IDTA no longer provided Appropriate Safeguards, but no other Processing;
 - 9.2.2 agree a change to Part one: Tables or Part two: Extra Protection Clauses which will maintain the Appropriate Safeguards (in accordance with Section 5); and
 - 9.2.3 where a change to Part one: Tables or Part two: Extra Protection Clauses which maintains the Appropriate Safeguards cannot be agreed, the Exporter must end this IDTA by written notice on the Importer.

10. The ICO

- 10.1 Each Party agrees to comply with any reasonable requests made by the ICO in relation to this IDTA or its Processing of the Transferred Data.
- 10.2 The Exporter will provide a copy of any TRA, the Importer Information and this IDTA to the ICO, if the ICO requests.
- 10.3 The Importer will provide a copy of any Importer Information and this IDTA to the ICO, if the ICO requests.

The Exporter

11. Exporter's obligations

- 11.1 The Exporter agrees that UK Data Protection Laws apply to its Processing of the Transferred Data, including transferring it to the Importer.
- 11.2 The Exporter must:

- 11.2.1 comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;
 - 11.2.2 comply with the Linked Agreement as it relates to its transferring the Transferred Data to the Importer; and
 - 11.2.3 carry out reasonable checks on the Importer's ability to comply with this IDTA, and take appropriate action including under Section 9.2, Section 29 or Section 30, if at any time it no longer considers that the Importer is able to comply with this IDTA or to provide Appropriate Safeguards.
- 11.3 The Exporter must comply with all its obligations in the IDTA, including any in the Security Requirements, and any Extra Protection Clauses and any Commercial Clauses.
- 11.4 The Exporter must co-operate with reasonable requests of the Importer to pass on notices or other information to and from Relevant Data Subjects or any Third Party Controller where it is not reasonably practical for the Importer to do so. The Exporter may pass these on via a third party if it is reasonable to do so.
- 11.5 The Exporter must co-operate with and provide reasonable assistance to the Importer, so that the Importer is able to comply with its obligations to the Relevant Data Subjects under Local Law and this IDTA.

The Importer

12. General Importer obligations

- 12.1 The Importer must:
- 12.1.1 only Process the Transferred Data for the Purpose;
 - 12.1.2 comply with all its obligations in the IDTA, including in the Security Requirements, any Extra Protection Clauses and any Commercial Clauses;
 - 12.1.3 comply with all its obligations in the Linked Agreement which relate to its Processing of the Transferred Data;
 - 12.1.4 keep a written record of its Processing of the Transferred Data, which demonstrate its compliance with this IDTA, and provide this written record if asked to do so by the Exporter;
 - 12.1.5 if the Linked Agreement includes rights for the Exporter to obtain information or carry out an audit, provide the Exporter with the same rights in relation to this IDTA; and

12.1.6 if the ICO requests, provide the ICO with the information it would be required on request to provide to the Exporter under this Section 12.1 (including the written record of its Processing, and the results of audits and inspections).

12.2 The Importer must co-operate with and provide reasonable assistance to the Exporter and any Third Party Controller, so that the Exporter and any Third Party Controller are able to comply with their obligations under UK Data Protection Laws and this IDTA.

13. Importer's obligations if it is subject to the UK Data Protection Laws

13.1 If the Importer's Processing of the Transferred Data is subject to UK Data Protection Laws, it agrees that:

13.1.1 UK Data Protection Laws apply to its Processing of the Transferred Data, and the ICO has jurisdiction over it in that respect; and

13.1.2 it has and will comply with the UK Data Protection Laws in relation to the Processing of the Transferred Data.

13.2 If Section 13.1 applies and the Importer complies with Section 13.1, it does not need to comply with:

- Section 14 (Importer's obligations to comply with key data protection principles);
- Section 15 (What happens if there is an Importer Personal Data Breach);
- Section 15 (How Relevant Data Subjects can exercise their data subject rights); and
- Section 21 (How Relevant Data Subjects can exercise their data subject rights – if the Importer is the Exporter's Processor or Sub-Processor).

14. Importer's obligations to comply with key data protection principles

14.1 The Importer does not need to comply with this Section 14 if it is the Exporter's Processor or Sub-Processor.

14.2 The Importer must:

14.2.1 ensure that the Transferred Data it Processes is adequate, relevant and limited to what is necessary for the Purpose;

14.2.2 ensure that the Transferred Data it Processes is accurate and (where necessary) kept up to date, and (where appropriate

considering the Purposes) correct or delete any inaccurate Transferred Data it becomes aware of Without Undue Delay; and

14.2.3 ensure that it Processes the Transferred Data for no longer than is reasonably necessary for the Purpose.

15. What happens if there is an Importer Personal Data Breach

15.1 If there is an Importer Personal Data Breach, the Importer must:

15.1.1 take reasonable steps to fix it, including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again. If the Importer is the Exporter's Processor or Sub-Processor: these steps must comply with the Exporter's instructions and the Linked Agreement and be in co-operation with the Exporter and any Third Party Controller; and

15.1.2 ensure that the Security Requirements continue to provide (or are changed in accordance with this IDTA so they do provide) a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

15.2 If the Importer is a Processor or Sub-Processor: if there is an Importer Personal Data Breach, the Importer must:

15.2.1 notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

15.2.1.1 a description of the nature of the Importer Personal Data Breach;

15.2.1.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;

15.2.1.3 likely consequences of the Importer Personal Data Breach;

15.2.1.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;

15.2.1.5 contact point for more information; and

15.2.1.6 any other information reasonably requested by the Exporter,

- 15.2.2 if it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay; and
 - 15.2.3 assist the Exporter (and any Third Party Controller) so the Exporter (or any Third Party Controller) can inform Relevant Data Subjects or the ICO or any other relevant regulator or authority about the Importer Personal Data Breach Without Undue Delay.
- 15.3 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a risk to the rights or freedoms of any Relevant Data Subject the Importer must notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:
- 15.3.1 a description of the nature of the Importer Personal Data Breach;
 - 15.3.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;
 - 15.3.3 likely consequences of the Importer Personal Data Breach;
 - 15.3.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;
 - 15.3.5 contact point for more information; and
 - 15.3.6 any other information reasonably requested by the Exporter.

If it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay.

- 15.4 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a high risk to the rights or freedoms of any Relevant Data Subject, the Importer must inform those Relevant Data Subjects Without Undue Delay, except in so far as it requires disproportionate effort, and provided the Importer ensures that there is a public communication or similar measures whereby Relevant Data Subjects are informed in an equally effective manner.
- 15.5 The Importer must keep a written record of all relevant facts relating to the Importer Personal Data Breach, which it will provide to the Exporter and the ICO on request.

This record must include the steps it takes to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to

ensure that Security Requirements continue to provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

16. Transferring on the Transferred Data

- 16.1 The Importer may only transfer on the Transferred Data to a third party if it is permitted to do so in Table 2: Transfer Details Table, the transfer is for the Purpose, the transfer does not breach the Linked Agreement, and one or more of the following apply:
- 16.1.1 the third party has entered into a written contract with the Importer containing the same level of protection for Data Subjects as contained in this IDTA (based on the role of the recipient as controller or processor), and the Importer has conducted a risk assessment to ensure that the Appropriate Safeguards will be protected by that contract; or
 - 16.1.2 the third party has been added to this IDTA as a Party; or
 - 16.1.3 if the Importer was in the UK, transferring on the Transferred Data would comply with Article 46 UK GDPR; or
 - 16.1.4 if the Importer was in the UK transferring on the Transferred Data would comply with one of the exceptions in Article 49 UK GDPR; or
 - 16.1.5 the transfer is to the UK or an Adequate Country.
- 16.2 The Importer does not need to comply with Section 16.1 if it is transferring on Transferred Data and/or allowing access to the Transferred Data in accordance with Section 23 (Access Requests and Direct Access).

17. Importer's responsibility if it authorises others to perform its obligations

- 17.1 The Importer may sub-contract its obligations in this IDTA to a Processor or Sub-Processor (provided it complies with Section 16).
- 17.2 If the Importer is the Exporter's Processor or Sub-Processor: it must also comply with the Linked Agreement or be with the written consent of the Exporter.
- 17.3 The Importer must ensure that any person or third party acting under its authority, including a Processor or Sub-Processor, must only Process the Transferred Data on its instructions.
- 17.4 The Importer remains fully liable to the Exporter, the ICO and Relevant Data Subjects for its obligations under this IDTA where it has sub-contracted any obligations to its Processors and Sub-Processors, or authorised an employee or other person to perform them (and references

to the Importer in this context will include references to its Processors, Sub-Processors or authorised persons).

What rights do individuals have?

18. The right to a copy of the IDTA

18.1 If a Party receives a request from a Relevant Data Subject for a copy of this IDTA:

18.1.1 it will provide the IDTA to the Relevant Data Subject and inform the other Party, as soon as reasonably possible;

18.1.2 it does not need to provide copies of the Linked Agreement, but it must provide all the information from those Linked Agreements referenced in the Tables;

18.1.3 it may redact information in the Tables or the information provided from the Linked Agreement if it is reasonably necessary to protect business secrets or confidential information, so long as it provides the Relevant Data Subject with a summary of those redactions so that the Relevant Data Subject can understand the content of the Tables or the information provided from the Linked Agreement.

19. The right to Information about the Importer and its Processing

19.1 The Importer does not need to comply with this Section 19 if it is the Exporter's Processor or Sub-Processor.

19.2 The Importer must ensure that each Relevant Data Subject is provided with details of:

- the Importer (including contact details and the Importer Data Subject Contact);
- the Purposes; and
- any recipients (or categories of recipients) of the Transferred Data;

The Importer can demonstrate it has complied with this Section 19.2 if the information is given (or has already been given) to the Relevant Data Subjects by the Exporter or another party.

The Importer does not need to comply with this Section 19.2 in so far as to do so would be impossible or involve a disproportionate effort, in which case, the Importer must make the information publicly available.

19.3 The Importer must keep the details of the Importer Data Subject Contact up to date and publicly available. This includes notifying the Exporter in writing of any such changes.

19.4 The Importer must make sure those contact details are always easy to access for all Relevant Data Subjects and be able to easily communicate with Data Subjects in the English language Without Undue Delay.

20. How Relevant Data Subjects can exercise their data subject rights

20.1 The Importer does not need to comply with this Section 20 if it is the Exporter's Processor or Sub-Processor.

20.2 If an individual requests, the Importer must confirm whether it is Processing their Personal Data as part of the Transferred Data.

20.3 The following Sections of this Section 20, relate to a Relevant Data Subject's Personal Data which forms part of the Transferred Data the Importer is Processing.

20.4 If the Relevant Data Subject requests, the Importer must provide them with a copy of their Transferred Data:

20.4.1 Without Undue Delay (and in any event within one month);

20.4.2 at no greater cost to the Relevant Data Subject than it would be able to charge if it were subject to the UK Data Protection Laws;

20.4.3 in clear and plain English that is easy to understand; and

20.4.4 in an easily accessible form

together with

20.4.5 (if needed) a clear and plain English explanation of the Transferred Data so that it is understandable to the Relevant Data Subject; and

20.4.6 information that the Relevant Data Subject has the right to bring a claim for compensation under this IDTA.

20.5 If a Relevant Data Subject requests, the Importer must:

20.5.1 rectify inaccurate or incomplete Transferred Data;

20.5.2 erase Transferred Data if it is being Processed in breach of this IDTA;

20.5.3 cease using it for direct marketing purposes; and

- 20.5.4 comply with any other reasonable request of the Relevant Data Subject, which the Importer would be required to comply with if it were subject to the UK Data Protection Laws.
- 20.6 The Importer must not use the Transferred Data to make decisions about the Relevant Data Subject based solely on automated processing, including profiling (the "Decision-Making"), which produce legal effects concerning the Relevant Data Subject or similarly significantly affects them, except if it is permitted by Local Law and:
 - 20.6.1 the Relevant Data Subject has given their explicit consent to such Decision-Making; or
 - 20.6.2 Local Law has safeguards which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK; or
 - 20.6.3 the Extra Protection Clauses provide safeguards for the Decision-Making which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK.

21. How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter’s Processor or Sub-Processor

- 21.1 Where the Importer is the Exporter’s Processor or Sub-Processor: If the Importer receives a request directly from an individual which relates to the Transferred Data it must pass that request on to the Exporter Without Undue Delay. The Importer must only respond to that individual as authorised by the Exporter or any Third Party Controller.

22. Rights of Relevant Data Subjects are subject to the exemptions in the UK Data Protection Laws

- 22.1 The Importer is not required to respond to requests or provide information or notifications under Sections 18, 19, 20, 21 and 23 if:
 - 22.1.1 it is unable to reasonably verify the identity of an individual making the request; or
 - 22.1.2 the requests are manifestly unfounded or excessive, including where requests are repetitive. In that case the Importer may refuse the request or may charge the Relevant Data Subject a reasonable fee; or
 - 22.1.3 a relevant exemption would be available under UK Data Protection Laws, were the Importer subject to the UK Data Protection Laws.

If the Importer refuses an individual's request or charges a fee under Section 22.1.2 it will set out in writing the reasons for its refusal or charge, and inform the Relevant Data Subject that they are entitled to bring a claim for compensation under this IDTA in the case of any breach of this IDTA.

How to give third parties access to Transferred Data under Local Laws

23. Access requests and direct access

23.1 In this Section 23 an "Access Request" is a legally binding request (except for requests only binding by contract law) to access any Transferred Data and "Direct Access" means direct access to any Transferred Data by public authorities of which the Importer is aware.

23.2 The Importer may disclose any requested Transferred Data in so far as it receives an Access Request, unless in the circumstances it is reasonable for it to challenge that Access Request on the basis there are significant grounds to believe that it is unlawful.

23.3 In so far as Local Laws allow and it is reasonable to do so, the Importer will Without Undue Delay provide the following with relevant information about any Access Request or Direct Access: the Exporter; any Third Party Controller; and where the Importer is a Controller, any Relevant Data Subjects.

23.4 In so far as Local Laws allow, the Importer must:

23.4.1 make and keep a written record of Access Requests and Direct Access, including (if known): the dates, the identity of the requestor/accessor, the purpose of the Access Request or Direct Access, the type of data requested or accessed, whether it was challenged or appealed, and the outcome; and the Transferred Data which was provided or accessed; and

23.4.2 provide a copy of this written record to the Exporter on each Review Date and any time the Exporter or the ICO reasonably requests.

24. Giving notice

24.1 If a Party is required to notify any other Party in this IDTA it will be marked for the attention of the relevant Key Contact and sent by e-mail to the e-mail address given for the Key Contact.

24.2 If the notice is sent in accordance with Section 24.1, it will be deemed to have been delivered at the time the e-mail was sent, or if that time is outside of the receiving Party's normal business hours, the receiving

Party's next normal business day, and provided no notice of non-delivery or bounceback is received.

24.3 The Parties agree that any Party can update their Key Contact details by giving 14 days' (or more) notice in writing to the other Party.

25. General clauses

25.1 In relation to the transfer of the Transferred Data to the Importer and the Importer's Processing of the Transferred Data, this IDTA and any Linked Agreement:

25.1.1 contain all the terms and conditions agreed by the Parties; and

25.1.2 override all previous contacts and arrangements, whether oral or in writing.

25.2 If one Party made any oral or written statements to the other before entering into this IDTA (which are not written in this IDTA) the other Party confirms that it has not relied on those statements and that it will not have a legal remedy if those statements are untrue or incorrect, unless the statement was made fraudulently.

25.3 Neither Party may novate, assign or obtain a legal charge over this IDTA (in whole or in part) without the written consent of the other Party, which may be set out in the Linked Agreement.

25.4 Except as set out in Section 17.1, neither Party may sub contract its obligations under this IDTA without the written consent of the other Party, which may be set out in the Linked Agreement.

25.5 This IDTA does not make the Parties a partnership, nor appoint one Party to act as the agent of the other Party.

25.6 If any Section (or part of a Section) of this IDTA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity and enforceability of any other Section (or the rest of that Section) of this IDTA.

25.7 If a Party does not enforce, or delays enforcing, its rights or remedies under or in relation to this IDTA, this will not be a waiver of those rights or remedies. In addition, it will not restrict that Party's ability to enforce those or any other right or remedy in future.

25.8 If a Party chooses to waive enforcing a right or remedy under or in relation to this IDTA, then this waiver will only be effective if it is made in writing. Where a Party provides such a written waiver:

25.8.1 it only applies in so far as it explicitly waives specific rights or remedies;

- 25.8.2 it shall not prevent that Party from exercising those rights or remedies in the future (unless it has explicitly waived its ability to do so); and
- 25.8.3 it will not prevent that Party from enforcing any other right or remedy in future.

What happens if there is a breach of this IDTA?

26. Breaches of this IDTA

- 26.1 Each Party must notify the other Party in writing (and with all relevant details) if it:
 - 26.1.1 has breached this IDTA; or
 - 26.1.2 it should reasonably anticipate that it may breach this IDTA, and provide any information about this which the other Party reasonably requests.
- 26.2 In this IDTA “Significant Harmful Impact” means that there is more than a minimal risk of a breach of the IDTA causing (directly or indirectly) significant damage to any Relevant Data Subject or the other Party.

27. Breaches of this IDTA by the Importer

- 27.1 If the Importer has breached this IDTA, and this has a Significant Harmful Impact, the Importer must take steps Without Undue Delay to end the Significant Harmful Impact, and if that is not possible to reduce the Significant Harmful Impact as much as possible.
- 27.2 Until there is no ongoing Significant Harmful Impact on Relevant Data Subjects:
 - 27.2.1 the Exporter must suspend sending Transferred Data to the Importer;
 - 27.2.2 If the Importer is the Exporter’s Processor or Sub-Processor: if the Exporter requests, the importer must securely delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter); and
 - 27.2.3 if the Importer has transferred on the Transferred Data to a third party receiver under Section 16, and the breach has a Significant Harmful Impact on Relevant Data Subject when it is Processed by or on behalf of that third party receiver, the Importer must:
 - 27.2.3.1 notify the third party receiver of the breach and suspend sending it Transferred Data; and

27.2.3.2 if the third party receiver is the Importer's Processor or Sub-Processor: make the third party receiver securely delete all Transferred Data being Processed by it or on its behalf, or securely return it to the Importer (or a third party named by the Importer).

27.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Exporter must end this IDTA under Section 30.1.

28. Breaches of this IDTA by the Exporter

28.1 If the Exporter has breached this IDTA, and this has a Significant Harmful Impact, the Exporter must take steps Without Undue Delay to end the Significant Harmful Impact and if that is not possible to reduce the Significant Harmful Impact as much as possible.

28.2 Until there is no ongoing risk of a Significant Harmful Impact on Relevant Data Subjects, the Exporter must suspend sending Transferred Data to the Importer.

28.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Importer must end this IDTA under Section 30.1.

Ending the IDTA

29. How to end this IDTA without there being a breach

29.1 The IDTA will end:

29.1.1 at the end of the Term stated in Table 2: Transfer Details; or

29.1.2 if in Table 2: Transfer Details, the Parties can end this IDTA by providing written notice to the other: at the end of the notice period stated;

29.1.3 at any time that the Parties agree in writing that it will end; or

29.1.4 at the time set out in Section 29.2.

29.2 If the ICO issues a revised Approved IDTA under Section 5.4, if any Party selected in Table 2 "Ending the IDTA when the Approved IDTA changes", will as a direct result of the changes in the Approved IDTA have a substantial, disproportionate and demonstrable increase in:

29.2.1 its direct costs of performing its obligations under the IDTA; and/or

29.2.2 its risk under the IDTA,

and in either case it has first taken reasonable steps to reduce that cost or risk so that it is not substantial and disproportionate, that Party may end the IDTA at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved IDTA.

30. How to end this IDTA if there is a breach

30.1 A Party may end this IDTA immediately by giving the other Party written notice if:

30.1.1 the other Party has breached this IDTA and this has a Significant Harmful Impact. This includes repeated minor breaches which taken together have a Significant Harmful Impact, and

30.1.1.1 the breach can be corrected so there is no Significant Harmful Impact, and the other Party has failed to do so Without Undue Delay (which cannot be more than 14 days of being required to do so in writing); or

30.1.1.2 the breach and its Significant Harmful Impact cannot be corrected;

30.1.2 the Importer can no longer comply with Section 8.3, as there are Local Laws which mean it cannot comply with this IDTA and this has a Significant Harmful Impact.

31. What must the Parties do when the IDTA ends?

31.1 If the parties wish to bring this IDTA to an end or this IDTA ends in accordance with any provision in this IDTA, but the Importer must comply with a Local Law which requires it to continue to keep any Transferred Data then this IDTA will remain in force in respect of any retained Transferred Data for as long as the retained Transferred Data is retained, and the Importer must:

31.1.1 notify the Exporter Without Undue Delay, including details of the relevant Local Law and the required retention period;

31.1.2 retain only the minimum amount of Transferred Data it needs to comply with that Local Law, and the Parties must ensure they maintain the Appropriate Safeguards, and change the Tables and Extra Protection Clauses, together with any TRA to reflect this; and

31.1.3 stop Processing the Transferred Data as soon as permitted by that Local Law and the IDTA will then end and the rest of this Section 29 will apply.

31.2 When this IDTA ends (no matter what the reason is):

31.2.1 the Exporter must stop sending Transferred Data to the Importer;
and

31.2.2 if the Importer is the Exporter's Processor or Sub-Processor: the Importer must delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter), as instructed by the Exporter;

31.2.3 if the Importer is a Controller and/or not the Exporter's Processor or Sub-Processor: the Importer must securely delete all Transferred Data.

31.2.4 the following provisions will continue in force after this IDTA ends (no matter what the reason is):

- **Section 1** (This IDTA and Linked Agreements);
- **Section 2** (Legal Meaning of Words);
- **Section 6** (Understanding this IDTA);
- **Section 7** (Which laws apply to this IDTA);
- **Section 10** (The ICO);
- Sections 11.1 and 11.4 (Exporter's obligations);
- Sections 12.1.2, 12.1.3, 12.1.4, 12.1.5 and 12.1.6 (General Importer obligations);
- Section 13.1 (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 17** (Importer's responsibility if it authorised others to perform its obligations);
- **Section 24** (Giving notice);
- **Section 25** (General clauses);
- **Section 31** (What must the Parties do when the IDTA ends);
- **Section 32** (Your liability);
- **Section 33** (How Relevant Data Subjects and the ICO may bring legal claims);
- **Section 34** (Courts legal claims can be brought in);
- **Section 35** (Arbitration); and

- **Section 36** (Legal Glossary).

How to bring a legal claim under this IDTA

32. Your liability

- 32.1 The Parties remain fully liable to Relevant Data Subjects for fulfilling their obligations under this IDTA and (if they apply) under UK Data Protection Laws.
- 32.2 Each Party (in this Section, "Party One") agrees to be fully liable to Relevant Data Subjects for the entire damage suffered by the Relevant Data Subject, caused directly or indirectly by:
- 32.2.1 Party One's breach of this IDTA; and/or
 - 32.2.2 where Party One is a Processor, Party One's breach of any provisions regarding its Processing of the Transferred Data in the Linked Agreement;
 - 32.2.3 where Party One is a Controller, a breach of this IDTA by the other Party if it involves Party One's Processing of the Transferred Data (no matter how minimal)
- in each case unless Party One can prove it is not in any way responsible for the event giving rise to the damage.
- 32.3 If one Party has paid compensation to a Relevant Data Subject under Section 32.2, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party's responsibility for the damage, so that the compensation is fairly divided between the Parties.
- 32.4 The Parties do not exclude or restrict their liability under this IDTA or UK Data Protection Laws, on the basis that they have authorised anyone who is not a Party (including a Processor) to perform any of their obligations, and they will remain responsible for performing those obligations.

33. How Relevant Data Subjects and the ICO may bring legal claims

- 33.1 The Relevant Data Subjects are entitled to bring claims against the Exporter and/or Importer for breach of the following (including where their Processing of the Transferred Data is involved in a breach of the following by either Party):
- **Section 1** (This IDTA and Linked Agreements);
 - **Section 3** (You have provided all the information required by Part one: Tables and Part two: Extra Protection Clauses);
 - **Section 8** (The Appropriate Safeguards);

- **Section 9** (Reviews to ensure the Appropriate Safeguards continue);
- **Section 11** (Exporter's obligations);
- **Section 12** (General Importer Obligations);
- **Section 13** (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 14** (Importer's obligations to comply with key data protection laws);
- **Section 15** (What happens if there is an Importer Personal Data Breach);
- **Section 16** (Transferring on the Transferred Data);
- **Section 17** (Importer's responsibility if it authorises others to perform its obligations);
- **Section 18** (The right to a copy of the IDTA);
- **Section 19** (The Importer's contact details for the Relevant Data Subjects);
- **Section 20** (How Relevant Data Subjects can exercise their data subject rights);
- **Section 21** (How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor);
- **Section 23** (Access Requests and Direct Access);
- **Section 26** (Breaches of this IDTA);
- **Section 27** (Breaches of this IDTA by the Importer);
- **Section 28** (Breaches of this IDTA by the Exporter);
- **Section 30** (How to end this IDTA if there is a breach);
- **Section 31** (What must the Parties do when the IDTA ends); and
- any other provision of the IDTA which expressly or by implication benefits the Relevant Data Subjects.

33.2 The ICO is entitled to bring claims against the Exporter and/or Importer for breach of the following Sections: Section 10 (The ICO), Sections 11.1 and 11.2 (Exporter's obligations), Section 12.1.6 (General Importer obligations) and Section 13 (Importer's obligations if it is subject to UK Data Protection Laws).

- 33.3 No one else (who is not a Party) can enforce any part of this IDTA (including under the Contracts (Rights of Third Parties) Act 1999).
- 33.4 The Parties do not need the consent of any Relevant Data Subject or the ICO to make changes to this IDTA, but any changes must be made in accordance with its terms.
- 33.5 In bringing a claim under this IDTA, a Relevant Data Subject may be represented by a not-for-profit body, organisation or association under the same conditions set out in Article 80(1) UK GDPR and sections 187 to 190 of the Data Protection Act 2018.

34. Courts legal claims can be brought in

- 34.1 The courts of the UK country set out in Table 2: Transfer Details have non-exclusive jurisdiction over any claim in connection with this IDTA (including non-contractual claims).
- 34.2 The Exporter may bring a claim against the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.
- 34.3 The Importer may only bring a claim against the Exporter in connection with this IDTA (including non-contractual claims) in the courts of the UK country set out in the Table 2: Transfer Details
- 34.4 Relevant Data Subjects and the ICO may bring a claim against the Exporter and/or the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.
- 34.5 Each Party agrees to provide to the other Party reasonable updates about any claims or complaints brought against it by a Relevant Data Subject or the ICO in connection with the Transferred Data (including claims in arbitration).

35. Arbitration

- 35.1 Instead of bringing a claim in a court under Section 34, any Party, or a Relevant Data Subject may elect to refer any dispute arising out of or in connection with this IDTA (including non-contractual claims) to final resolution by arbitration under the Rules of the London Court of International Arbitration, and those Rules are deemed to be incorporated by reference into this Section 35.
- 35.2 The Parties agree to submit to any arbitration started by another Party or by a Relevant Data Subject in accordance with this Section 35.

- 35.3 There must be only one arbitrator. The arbitrator (1) must be a lawyer qualified to practice law in one or more of England and Wales, or Scotland, or Northern Ireland and (2) must have experience of acting or advising on disputes relating to UK Data Protection Laws.
- 35.4 London shall be the seat or legal place of arbitration. It does not matter if the Parties selected a different UK country as the 'primary place for legal claims to be made' in Table 2: Transfer Details.
- 35.5 The English language must be used in the arbitral proceedings.
- 35.6 English law governs this Section 35. This applies regardless of whether or not the parties selected a different UK country's law as the 'UK country's law that governs the IDTA' in Table 2: Transfer Details.

36. Legal Glossary

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Access Request	As defined in Section 23, as a legally binding request (except for requests only binding by contract law) to access any Transferred Data.
Adequate Country	<p>A third country, or:</p> <ul style="list-style-type: none"> • a territory; • one or more sectors or organisations within a third country; • an international organisation; <p>which the Secretary of State has specified by regulations provides an adequate level of protection of Personal Data in accordance with Section 17A of the Data Protection Act 2018.</p>
Appropriate Safeguards	The standard of protection over the Transferred Data and of the Relevant Data Subject's rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved IDTA	The template IDTA A1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
	Act 2018 on 2 February 2022, as it is revised under Section 5.4.
Commercial Clauses	The commercial clauses set out in Part three.
Controller	As defined in the UK GDPR.
Damage	All material and non-material loss and damage.
Data Subject	As defined in the UK GDPR.
Decision-Making	As defined in Section 20.6, as decisions about the Relevant Data Subjects based solely on automated processing, including profiling, using the Transferred Data.
Direct Access	As defined in Section 23 as direct access to any Transferred Data by public authorities of which the Importer is aware.
Exporter	The exporter identified in Table 1: Parties & Signature.
Extra Protection Clauses	The clauses set out in Part two: Extra Protection Clauses.
ICO	The Information Commissioner.
Importer	The importer identified in Table 1: Parties & Signature.
Importer Data Subject Contact	The Importer Data Subject Contact identified in Table 1: Parties & Signature, which may be updated in accordance with Section 19.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Importer Information	As defined in Section 8.3.1, as all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including for the Exporter to carry out any TRA.
Importer Personal Data Breach	A 'personal data breach' as defined in UK GDPR, in relation to the Transferred Data when Processed by the Importer.
Linked Agreement	The linked agreements set out in Table 2: Transfer Details (if any).
Local Laws	Laws which are not the laws of the UK and which bind the Importer.
Mandatory Clauses	Part four: Mandatory Clauses of this IDTA.
Notice Period	As set out in Table 2: Transfer Details.
Party/Parties	The parties to this IDTA as set out in Table 1: Parties & Signature.
Personal Data	As defined in the UK GDPR.
Personal Data Breach	As defined in the UK GDPR.
Processing	As defined in the UK GDPR. When the IDTA refers to Processing by the Importer, this includes where a third party Sub-Processor of the Importer is Processing on the Importer's behalf.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Processor	As defined in the UK GDPR.
Purpose	The 'Purpose' set out in Table 2: Transfer Details, including any purposes which are not incompatible with the purposes stated or referred to.
Relevant Data Subject	A Data Subject of the Transferred Data.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR
Review Dates	The review dates or period for the Security Requirements set out in Table 2: Transfer Details, and any review dates set out in any revised Approved IDTA.
Significant Harmful Impact	As defined in Section 26.2 as where there is more than a minimal risk of the breach causing (directly or indirectly) significant harm to any Relevant Data Subject or the other Party.
Special Category Data	As described in the UK GDPR, together with criminal conviction or criminal offence data.
Start Date	As set out in Table 1: Parties and signature.
Sub-Processor	A Processor appointed by another Processor to Process Personal Data on its behalf. This includes Sub-Processors of any level, for example a Sub-Sub-Processor.
Tables	The Tables set out in Part one of this IDTA.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Term	As set out in Table 2: Transfer Details.
Third Party Controller	The Controller of the Transferred Data where the Exporter is a Processor or Sub-Processor If there is not a Third Party Controller this can be disregarded.
Transfer Risk Assessment or TRA	A risk assessment in so far as it is required by UK Data Protection Laws to demonstrate that the IDTA provides the Appropriate Safeguards
Transferred Data	Any Personal Data which the Parties transfer, or intend to transfer under this IDTA, as described in Table 2: Transfer Details
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in Section 3 of the Data Protection Act 2018.
Without Undue Delay	Without undue delay, as that phrase is interpreted in the UK GDPR.

Alternative Part 4 Mandatory Clauses:

Mandatory Clauses	Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.
--------------------------	--

Annex 4 (c) LSE Data Sharing Minimum Standards

This document outlines the minimum standards around the processing of LSE data outside the European Economic Area (EEA) by individual consultants that are employed by, or contracted to, the LSE.

Any data in relation to LSE's business or research work is owned by the LSE, regardless of whether the data are processed by LSE members or not.

As the 'Data Controller' of such data the LSE is legally obligated to implement appropriate technical and organisational measures around any personal data involved. Any breach of the personal data can subject the School to a financial fine of up to 20 Million Euros or 4% of global turnover whichever is higher, under the General Data Protection Regulation (GDPR) and UK Data Protection Act 2018 (DPA 2018) (hereinafter referred to in this Policy as 'Data Protection legislation').

Purpose

The primary purposes of this Minimum Standard are to:

1. Provide the minimum requirements around the data processing outside the EEA by the individual consultant, either directly reemployed by, or contracted to, the LSE.
2. Protect the confidentiality, integrity, and availability of LSE data.
3. Ensure that the School as the Data Controller meets its legal duties under the Data Protection legislation.

NOTE: where there are contractual requirements that exceed or conflict with the minimum standards outlined below, the contractual requirements take precedence.

Scope

This Minimum Standard is intended for all processing of LSE data by an individual consultant that is employed by or contracted to the LSE.

This Minimum Standard does NOT apply to consultants that represent an external organisation undertaking contractual work for the LSE.

Accompanying documents

This Minimum Standard is supported by the following documents:

The Information Security Policy and Information Classification Standard, which outline how to classify data and how data of different categories must be secured.

Data Protection Policy, which provides an overview of data protection requirements under the Data Protection legislation.

Device Level Security Minimum Standards, which provides baseline information security around device that's used to process LSE data.
Minimum Standards

Data storage inside the EEA

Where LSE is commissioning an individual consultant to carry out LSE business or research work that involves LSE data, the consultant is considered as LSE's 'Data Processor', where LSE remains as the 'Data Controller'.

Any personal data that are processed by the consultant should be stored in UK or EEA where possible and practicable. This can be achieved via:

- If the consultant is not bound by a formal employment contract, a permanent LSE employee who's responsible for the research project can create a SharePoint or One Drive for Business external collaborator account for the consultant.
- If the consultant is bound by a formal employment contract and is authorised by the Manager of the Department employing such consultant to have a standard network account, the data can be stored

in SharePoint, One Drive for Business, H: space, departmental shared folder, or any other LSE-provided storage space.

Additionally, any personal device that's used to access such data shall observe LSE's Device Level Security Minimum Standards.

Data storage outside the EEA

In cases where data must be stored and processed outside the EEA, following minimum standards must be met in addition to a binding Data Processing Agreement.

Desktop level security

Any desktop that's used to access the personal data must meet the following:

- Only authorised personnel have access to the desktop.
- Access to the desktop must require an identifiable user ID, and a complex password; such password must at least be:
 - 15 characters long
 - Contain at least one upper case letter and at least one lower case letter.
 - Contain at least one number or punctuation character.
 - Avoid international (non-ASCII) characters.
 - Not be a dictionary word.
- Any desktop level default password must be removed.
- The desktop is equipped with up-to-date Anti-virus and is scanned regularly.
- The Operating System and other software on the desktop are up-to-date and fully patched.
- Software firewall must be enabled.
- Apply a screen saver that automatically locks after 5 – 15 minutes' inactivity.
- The desktop must be in a place with adequate physical security protections, if not then the desktop must be encrypted at the hard drive level.

Mobile device security

Any mobile device that's used to access the personal data must meet the following:

- Any mobile device including laptop, tablet, smart phone, externa storage device, that's used to store, access, process, share the LSE data must have full drive encryption applied.
 - The encryption key – if managed by the user – should be at least:
 - 15 characters long
 - Contain at least one upper case letter and at least one lower case letter.
 - Contain at least one number or punctuation character.
 - Avoid international (non-ASCII) characters.
 - Not be a dictionary word.
 - Strong logon password and should be at least:
 - 15 characters long (or 6-digit PIN for phones)
 - Contain at least one upper case letter and at least one lower case letter.
 - Contain at least one number or punctuation character.
 - Avoid international (non-ASCII) characters.
 - Not a dictionary word
 - The device actively operates anti-virus software with regular scans.
 - The device actively operates a software firewall (e.g. enable the built-in firewall option in the Operating System)
 - Keep the Operating Systems up to date by installing security patches as soon as they are released, and no later than 14 days after they are released.
 - Keep other software up to date by implementing security patches as soon as they are released, and no later than 14 days after they are released.
 - Apply a screen saver that automatically locks after 5 – 10 minutes' inactivity.
- Preferably apply a 'privacy screen' for laptop if working with personal or otherwise sensitive data in public area (e.g. 3M laptop privacy screen).
 - Any external storage device if containing personally identifying data must be encrypted.

Data backup

- Suitable data backup arrangement should be in place.
- Any storage location for the data backup must be applied with the equivalent level of controls as described above.

Access permission to the data

- 'Least privilege' and 'need to know' must be observed, i.e. only the right personnel have the right access to the right resources.
- Regular permission review is carried out to make sure only the right people have access to the right resources.

Physical format of data

Physical format of identifying data is kept in a locked file cabinet and are securely destroyed when no longer in use.