MODEL SERVICES AGREEMENT COMBINED SCHEDULES

CON_13706

MODEL AGREEMENT FOR SERVICES

SCHEDULES, ANNEXES AND PARTS

SCHEDULE 8.6 SERVICE CONTINUITY PLAN AND CORPORATE RESOLUTION PLANNING
PART A: SERVICE CONTINUITY PLAN
PART B: CORPORATE RESOLUTION PLANNING
ANNEX 1: GROUP STRUCTURE INFORMATION AND RESOLUTION COMMENTARY
ANNEX 2: UK PUBLIC SECTOR / CNI CONTRACT INFORMATION

SCHEDULE 8.7 CONDUCT OF CLAIMS

SCHEDULE 9.1 STAFF TRANSFER
PART A: NOT USED
PART B: TRANSFERRING FORMER SUPPLIER EMPLOYEES AT COMMENCEMENT OF SERVICES
PART C: NOT USED
PART D: NOT USED
PART E: EMPLOYMENT EXIT PROVISIONS
ANNEX E1: LIST OF NOTIFIED SUB-CONTRACTORS
ANNEX E2: STAFFING INFORMATION

SCHEDULE 9.2 KEY PERSONNEL

SCHEDULE 10 NOT USED

SCHEDULE 11 PROCESSING PERSONAL DATA
ANNEX 1: JOINT CONTROLLER AGREEMENT
ANNEX 2: NOT USED
ANNEX 3: NOT USED
ANNEX 4: USER JOURNEYS

SCHEDULE 12 – ASSET REGISTER

MODEL AGREEMENT FOR SERVICES SCHEDULES

SCHEDULE 1

DEFINITIONS

Definitions

1.1 Unless otherwise provided or the context otherwise requires the following expressions shall have the meanings set out below.

"Accounting Reference Date"	means in each year the date to which the Supplier prepares its annual audited financial statements;
"Affected Party"	the Party seeking to claim relief in respect of a Force Majeure Event;
"Affiliate"	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time;
"Annual Revenue"	means, for the purposes of determining whether an entity is a Public Sector Dependent Supplier, the audited consolidated aggregate revenue (including share of revenue of joint ventures and Associates) reported by the Supplier or, as appropriate, the Supplier Group in its most recent published accounts, subject to the following methodology: (a) figures for accounting periods of other than 12 months should be scaled pro rata to produce a proforma figure for a 12 month period; and (b) where the Supplier, the Supplier Group and/or their joint ventures and Associates report in a foreign currency, revenue should be converted to British Pound Sterling at the closing exchange rate on the Accounting Reference Date;
"Approved Sub-Licensee"	any of the following: (a) a Central Government Body; (b) any third party providing services to a Central Government Body; and/or (c) any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Authority;
"Assets"	all assets and rights used by the Supplier to provide the Services in accordance with this Agreement but excluding the Authority Assets;

"Associated Person"	has the meaning given to it in Section 44(4) of the Criminal Finances Act 2017;
"Associates"	means, in relation to an entity, an undertaking in which the entity owns, directly or indirectly, between 20% and 50% of the voting rights and exercises a degree of control sufficient for the undertaking to be treated as an associate under generally accepted accounting principles;
"Assurance"	means written confirmation from a Relevant Authority to the Supplier that the CRP Information is approved by the Relevant Authority;
"Audit"	any exercise by the Authority of its Audit Rights pursuant to Clause 12 (*Records, Reports, Audit and Open Book Data*) and Schedule 7.5 (*Financial Reports and Audit Rights*);
"Audit Agents"	(a) the Authority's internal and external auditors; (b) the Authority's statutory or regulatory auditors; (c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; (d) HM Treasury or the Cabinet Office; (e) any party formally appointed by the Authority to carry out audit or similar review functions; and (f) successors or assigns of any of the above;
"Audit Rights"	the audit and access rights referred to in Schedule 7.5 (*Financial Reports and Audit Rights*);
"Authority Assets"	the Authority Materials, the Authority infrastructure and any other data, software, assets, equipment or other property owned by and/or licensed or leased to the Authority and which is or may be used in connection with the provision or receipt of the Services;
"Authority Background IPRs"	(a) IPRs owned by the Authority before the Effective Date, including IPRs contained in any of the Authority's Know-How, documentation, processes and procedures; (b) IPR owned by the Authority before the Effective Date in the items listed in the Asset Registers

(c) IPRs created by the Authority independently of this Agreement; and/or

(d) Crown Copyright which is not available to the Supplier otherwise than under this Agreement;

but excluding IPRs owned by the Authority subsisting in the Authority Software;

"Authority Cause" any material breach by the Authority of any of the Authority Responsibilities, except to the extent that such breach is:

(a) the result of any act or omission by the Authority to which the Supplier has given its prior consent; or

(b) caused by the Supplier, any Sub-contractor or any Supplier Personnel;

"Authority Data"

(c) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are:

(i) supplied to the Supplier by or on behalf of the Authority; and/or

(ii) which the Supplier is required to generate, process, store or transmit pursuant to this Agreement; or

(d) any Personal Data for which the Authority is the Data Controller;

"Authority Materials" the Authority Data together with any materials, documentation, information, programs and codes supplied by the Authority to the Supplier, the IPRs in which:

(a) are owned or used by or on behalf of the Authority; and

(b) are or may be used in connection with the provision or receipt of the Services,

but excluding any Project Specific IPRs, Supplier Software, Third Party Software and Documentation relating to Supplier Software or Third Party Software;

"Authority Representative"	the representative appointed by the Authority pursuant to Clause 11.4 (*Representatives*);
"Authority Requirements"	the requirements of the Authority set out in Schedules Schedule 2 (*Services Description*), Schedule 2.2 (*Performance Indicators*), Schedule 2.3 (*Standards*), Schedule 2.4 (*Security Management*), Schedule 2.5 (*Insurance Requirements*), Schedule 8.4 (*Reports and Records Provisions*), Schedule 8.5 (*Exit Management*) and Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);
"Authority Responsibilities"	the responsibilities of the Authority specified in Schedule 3 (*Authority Responsibilities*);
"Asset Registers"	means the spreadsheets contained at Schedule 12 (Asset Registers);
"Balanced Scorecard Report"	has the meaning given in Paragraph 1.1(b) of Part B of Schedule 2.2 (*Performance Levels*);
"Security Requirements"	the Authority's security requirements, the current copy of which is contained in Annex 1 of Schedule 2.4 (*Security Management*), as updated from time to time by the Authority and notified to the Supplier;
"Board"	means the Supplier's board of directors;
"Breakage Costs Payment"	has the meaning given in Schedule 7.2 (*Payments on Termination*);
"Cabinet Office Markets and Suppliers Team"	means the UK Government's team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function;
"Central Government Body"	a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: (a) Government Department; (b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); (c) Non-Ministerial Department; or

	(d) Executive Agency;
"Change"	any change to this Agreement;
"Change Authorisation Note"	a form setting out an agreed Contract Change which shall be substantially in the form of Annex 2 of Schedule 8.2 (*Change Control Procedure*);
"Change Control Procedure"	the procedure for changing this Agreement set out in Schedule 8.2 (*Change Control Procedure*);
"Change in Law"	any change in Law which impacts on the performance of the Services which comes into force after the Effective Date;
"Change Request"	a written request for a Contract Change substantially in the form of Annex 1 of Schedule 8.2 (*Change Control Procedure*);
"Charges"	the charges for the provision of the Services set out in or otherwise calculated in accordance with Schedule 7 (*Charges and Invoicing*);
"Class 1 Transaction"	has the meaning set out in the listing rules issued by the UK Listing Authority;
"CNI"	means Critical National Infrastructure;
"Commercially Sensitive Information"	the information listed in Schedule 4.2 (*Commercially Sensitive Information*) comprising the information of a commercially sensitive nature which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss;
"Comparable Supply"	the supply of services to another customer of the Supplier that are the same or similar to any of the Services;
"Confidential Information"	(a) Information, including all Personal Data, which (however it is conveyed) is provided by the Disclosing Party pursuant to or in anticipation of this Agreement that relates to: (i) the Disclosing Party Group; or (ii) the operations, business, affairs, developments, intellectual property rights,

trade secrets, know-how and/or personnel of the Disclosing Party Group;

(b) other Information provided by the Disclosing Party pursuant to or in anticipation of this Agreement that is clearly designated as being confidential or equivalent or that ought reasonably to be considered to be confidential (whether or not it is so marked) which comes (or has come) to the Recipient's attention or into the Recipient's possession in connection with this Agreement;

(c) discussions, negotiations, and correspondence between the Disclosing Party or any of its directors, officers, employees, consultants or professional advisers and the Recipient or any of its directors, officers, employees, consultants and professional advisers in connection with this Agreement and all matters arising therefrom; and

(d) Information derived from any of the above,

but not including any Information which:

(i) was in the possession of the Recipient without obligation of confidentiality prior to its disclosure by the Disclosing Party;

(ii) the Recipient obtained on a non-confidential basis from a third party who is not, to the Recipient's knowledge or belief, bound by a confidentiality agreement with the Disclosing Party or otherwise prohibited from disclosing the information to the Recipient;

(iii) was already generally available and in the public domain at the time of disclosure otherwise than by a breach of this Agreement or breach of a duty of confidentiality;

(iv) was independently developed without access to the Confidential Information; or

(v) relates to the Supplier's:

(1) performance under this Agreement; or

(2) failure to pay any Sub-contractor as required pursuant to Clause 15.15(a) (*Supply Chain Protection*);

"Contract Change"	any change to this Agreement other than an Operational Change;
"Contract Finder"	the online government portal which allows suppliers to search for information about contracts worth over [redacted] (excluding VAT) as prescribed by Part 4 of the Public Contract Regulations 2015;
"Contract Year"	(a) a period of 12 months commencing on the Services Commencement Date ; and (b) thereafter a period of 7 months commencing on the anniversary of the Services Commencement Date; provided that the final Contract Year shall end on the expiry or termination of the Term;
"Control"	the possession by person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and "**Controls**" and "**Controlled**" shall be interpreted accordingly;
"Controller"	has the meaning given in the UK GDPR;
"Corporate Change Event"	means: (a) any change of Control of the Supplier or a Parent Undertaking of the Supplier; (b) any change of Control of any member of the Supplier Group which, in the reasonable opinion of the Authority, could have a material adverse effect on the Services; (c) any change to the business of the Supplier or any member of the Supplier Group which, in the reasonable opinion of the Authority, could have a material adverse effect on the Services; (d) a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the London Stock Exchange plc; (e) an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking

place in respect of the Supplier or any Parent Undertaking of the Supplier;

(f) payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the Net Asset Value of the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any 12 month period;

(g) an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group;

(h) any member of the Supplier Group stopping payment of its debts generally or becoming unable to pay its debts within the meaning of section 123(1) of the Insolvency Act 1986 or any member of the Supplier Group ceasing to carry on all or substantially all its business, or any compromise, composition, arrangement or agreement being made with creditors of any member of the Supplier Group;

(i) the appointment of a receiver, administrative receiver or administrator in respect of or over all or a material part of the undertaking or assets of any member of the Supplier Group; and/or

(j) any process or events with an effect analogous to those in paragraphs (e) to (g) inclusive above occurring to a member of the Supplier Group in a jurisdiction outside England and Wales;

"Corporate Resolution Planning Information" means, together, the:

(a) Group Structure Information and Resolution Commentary; and

(b) UK Public Sector and CNI Contract Information;

"Costs" has the meaning given in Schedule 7 (*Charges and Invoicing*);

"Critical National Infrastructure" means those critical elements of UK national infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

(a) major detrimental impact on the availability, integrity or delivery of essential services –

	including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or (b) significant impact on the national security, national defence, or the functioning of the UK;
"Critical Service Contract"	means the overall status of the Services provided under this Agreement as determined by the Authority and specified in paragraph 10.1 of Part B to Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);
"CRP Information"	means the Corporate Resolution Planning Information;
"CRTPA"	the Contracts (Rights of Third Parties) Act 1999;
"Data Loss Event"	any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach;
"Data Protection Impact Assessment"	an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;
"Data Protection Legislation"	(a) the UK GDPR, as amended from time to time (b) the DPA 2018 to the extent that it relates to processing of personal data and privacy; (c) all applicable Law about the processing of personal data and privacy;
"Data Subject"	has the meaning given in the UK GDPR;
"Data Subject Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to their Personal Data;
"Deductions"	all Service Credits, or any other deduction which is paid or payable to the Authority under this Agreement;
"Default"	any breach of the obligations of the relevant Party (including abandonment of this Agreement in breach of its terms, repudiatory breach or breach of a

	fundamental term) or any other default, act, omission, negligence or statement: (a) in the case of the Authority, of its employees, servants, agents; or (b) in the case of the Supplier, of its Sub-contractors or any Supplier Personnel, in connection with or in relation to the subject-matter of this Agreement and in respect of which such Party is liable to the other;
"Defect"	(a) any error, damage or defect in the manufacturing of a Deliverable; or (b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or (c) any failure of any Deliverable to provide the performance, features and functionality specified in the Authority Requirements or the Documentation (including any adverse effect on response times) or (d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the Authority Requirements or the Documentation (including any adverse effect on response times);
"Deliverable"	an item or feature delivered or to be delivered by the Supplier at any other stage during the performance of this Agreement;
"Dependent Parent Undertaking"	means any Parent Undertaking which provides any of its Subsidiary Undertakings and/or Associates, whether directly or indirectly, with any financial, trading, managerial or other assistance of whatever nature, without which the Supplier would be unable to continue the day to day conduct and operation of its business in the same manner as carried on at the time of entering into this Agreement, including for the avoidance of doubt the provision of the Services in accordance with the terms of this Agreement;
"Disclosing Party"	has the meaning given in Clause 22.1 (*Confidentiality*);

"Disclosing Party Group"	(a) where the Disclosing Party is the Supplier, the Supplier and any Affiliates of the Supplier; and (b) where the Disclosing Party is the Authority, the Authority and any Central Government Body with which the Authority or the Supplier interacts in connection with this Agreement;
"Dispute"	any dispute, difference or question of interpretation arising out of or in connection with this Agreement, including any dispute, difference or question of interpretation relating to the Services, failure to agree in accordance with the Change Control Procedure or any matter where this Agreement directs the Parties to resolve an issue by reference to the Dispute Resolution Procedure;
"Dispute Notice"	a written notice served by one Party on the other stating that the Party serving the notice believes that there is a Dispute;
"Dispute Resolution Procedure"	the dispute resolution procedure set out in Schedule 8.3 (*Dispute Resolution Procedure*);
"Documentation"	descriptions of the Services and Performance Indicators, details of the Supplier System (including (i) vendors and versions for off-the-shelf components and (ii) source code and build information for proprietary components), relevant design and development information, technical specifications of all functionality including those not included in standard manuals (such as those that modify system performance and access levels), configuration details, test scripts, user manuals, operating manuals, process definitions and procedures, and all such other documentation as: (a) is required to be supplied by the Supplier to the Authority under this Agreement; (b) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Authority to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide Services; (c) is required by the Supplier in order to provide the Services; and/or (d) has been or shall be generated for the purpose of providing the Services;

"DOTAS"	the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to national insurance contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868) made under section 132A of the Social Security Administration Act 1992;
"DPA"	the Data Protection Act 2018;
"Due Diligence Information"	any information supplied to the Supplier by or on behalf of the Authority prior to the Effective Date;
"Effective Date"	the Services Commencement Date;
"EIRs"	the Environmental Information Regulations 2004, together with any guidance and/or codes of practice issued by the Information Commissioner or any Central Government Body in relation to such Regulations;
"Emergency Maintenance"	ad hoc and unplanned maintenance provided by the Supplier where: (a) the Authority reasonably suspects that the IT Environment or the Services, or any part of the IT Environment or the Services, has or may have developed a fault, and notifies the Supplier of the same; or (b) the Supplier reasonably suspects that the IT Environment or the Services, or any part the IT Environment or the Services, has or may have developed a fault;
"Employee Liabilities"	all claims, actions, proceedings, orders, demands, complaints, investigations (save for any claims for personal injury which are covered by insurance) and any award, compensation, damages, tribunal awards, fine, loss, order, penalty, disbursement, payment made by way of settlement and costs, expenses and legal costs reasonably incurred in connection with a claim or investigation related to employment including in relation to the following:

(a) redundancy payments including contractual or enhanced redundancy costs, termination costs and notice payments;

(b) unfair, wrongful or constructive dismissal compensation;

(c) compensation for discrimination on grounds of sex, race, disability, age, religion or belief, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation or claims for equal pay;

(d) compensation for less favourable treatment of part-time workers or fixed term employees;

(e) outstanding employment debts and unlawful deduction of wages including any PAYE and national insurance contributions;

(f) employment claims whether in tort, contract or statute or otherwise;

(g) any investigation relating to employment matters by the Equality and Human Rights Commission or other enforcement, regulatory or supervisory body and of implementing any requirements which may arise from such investigation;

"Employment Regulations"	the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the Acquired Rights Directive;
"Estimated Year 1 Charges"	the estimated Charges payable by the Authority during the first Contract Year, as set out in the Pricing Model;
"Exit Management"	services, activities, processes and procedures to ensure a smooth and orderly transition of all or part of the Services from the Supplier to the Authority and/or a Replacement Supplier, as set out or referred to in Schedule 8.5 (*Exit Management*);
"Exit Plan"	the plan produced and updated by the Supplier during the Term in accordance with Paragraph 4 of Schedule 8.5 (*Exit Management*);
"Expedited Dispute Timetable"	the reduced timetable for the resolution of Disputes set out in Paragraph 3 of Schedule 8.3 (*Dispute Resolution Procedure*);

"Expert"	has the meaning given in Schedule 8.3 (*Dispute Resolution Procedure*);
"Expert Determination"	the process described in Paragraph 6 of Schedule 8.3 (*Dispute Resolution Procedure*);
"Financial Distress Event"	the occurrence of one or more of the events listed in Paragraph 3.1 of Schedule 7.4 (*Financial Distress*);
"Financial Distress Remediation Plan"	a plan setting out how the Supplier will ensure the continued performance and delivery of the Services in accordance with this Agreement in the event that a Financial Distress Event occurs;
"Financial Reports"	has the meaning given in Schedule 7.5 (*Financial Reports and Audit Rights*);
"Financial Transparency Objectives"	has the meaning given in Schedule 7.5 (*Financial Reports and Audit Rights*);
"FOIA"	the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time, together with any guidance and/or codes of practice issued by the Information Commissioner or any relevant Central Government Body in relation to such Act;
"Force Majeure Event"	any event outside the reasonable control of either Party affecting its performance of its obligations under this Agreement arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party, including riots, war or armed conflict, acts of terrorism, acts of government, local government or regulatory bodies, fire, flood, storm or earthquake, or other natural disaster but excluding any industrial dispute relating to the Supplier or the Supplier Personnel or any other failure in the Supplier's or a Sub-contractor's supply chain;
"Force Majeure Notice"	a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event;
"Former Supplier"	has the meaning given in Schedule 9 (*Staff Transfer*);

"GDPR"	means the UK GDPR;
"General Anti-Abuse Rule"	(a) the legislation in Part 5 of the Finance Act 2013; and (b) any future legislation introduced into Parliament to counteract tax advantages arising from abusive arrangements to avoid national insurance contributions;
"General Change in Law"	a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
"Good Industry Practice"	at any time the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would be reasonably expected at such time from a leading and expert supplier of services similar to the Services to a customer like the Authority, such supplier seeking to comply with its contractual obligations in full and complying with applicable Laws;
"Group Structure Information and Resolution Commentary"	means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 11 to 13 and Annex 1 of Part B of Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);
"Halifax Abuse Principle"	the principle explained in the CJEU Case C-255/02 Halifax and others;
"Health and Safety Policy"	the health and safety policy of the Authority and/or other relevant Central Government Body as provided to the Supplier on or before the Effective Date and as subsequently provided to the Supplier from time to time except any provision of any such subsequently provided policy that cannot be reasonably reconciled to ensuring compliance with applicable Law regarding health and safety;
"HMRC"	HM Revenue & Customs;
"Impact Assessment"	has the meaning given in Schedule 8.2 (*Change Control Procedure*);
"Indemnified Person"	the Authority and each and every person to whom the Authority (or any direct or indirect sub-licensee of the Authority) sub-licenses, assigns or novates any

Relevant IPRs or rights in Relevant IPRs in accordance with this Agreement;

"Independent Control" where a Controller has provided Personal Data to another Party which is neither a Processor or Joint Controller because the recipient itself determines the purposes and means of processing but does so separately from the Controller providing it with Personal Data;

"Information" all information of whatever nature, however conveyed and in whatever form, including in writing, orally, by demonstration, electronically and in a tangible, visual or machine-readable medium (including CD-ROM, magnetic and digital form);

"Insolvency Event" with respect to any person, means:

(a) that person 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:

(i) (being a company or a LLP) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986, or

(ii) (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986;

(b) that person commences negotiations with one or more of its creditors (using a voluntary arrangement, scheme of arrangement or otherwise) with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with one or more of its creditors or takes any step to obtain a moratorium pursuant to Section 1A and Schedule A1 of the Insolvency Act 1986 other than (in the case of a company, a LLP or a partnership) for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;

(c) another person becomes entitled to appoint a receiver over the assets of that person or a receiver is appointed over the assets of that person;

(d) a creditor or encumbrancer of that person attaches or takes possession of, or a distress, execution or other such process is levied or enforced on or sued against, the whole or any part of that person's assets and such attachment or process is not discharged within fourteen (14) days;

(e) that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business;

(f) where that person is a company, a LLP or a partnership:

(i) a petition is presented (which is not dismissed within fourteen (14) days of its service), a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of that person other than for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;

(ii) 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 filed at Court or given or if an administrator is appointed, over that person;

(iii) (being a company or a LLP) the holder of a qualifying floating charge over the assets of that person has become entitled to appoint or has appointed an administrative receiver; or

(iv) (being a partnership) the holder of an agricultural floating charge over the assets of that person has become entitled to appoint or has appointed an agricultural receiver; or

(g) any event occurs, or proceeding is taken, with respect to that person in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned above;

"Intellectual Property Rights" or **"IPRs"**

(a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor

topography rights, trade marks, rights in Internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information;

(b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and

(c) all other rights having equivalent or similar effect in any country or jurisdiction;

"Intervention Cause" has the meaning given in Clause 30.1 (*Remedial Adviser*);

"Intervention Notice" has the meaning given in Clause 30.1 (*Remedial Adviser*);

"Intervention Period" has the meaning given in Clause 30.2(c) (*Remedial Adviser*);

"Intervention Trigger Event"

(a) any event falling within limb (a), (b), (d), (e) or (f) of the definition of a Supplier Termination Event;

(b) a Default by the Supplier that is materially preventing or materially delaying the performance of the Services or any material part of the Services;

"IP Completion Day" has the meaning given to it in the European Union (Withdrawal Agreement) Act 2020;

"IPRs Claim" any claim against any Indemnified Person of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any Relevant IPRs save for any such claim to the extent that it is caused by any use by or on behalf of that Indemnified Person of any Relevant IPRs, in either case in combination with any item not supplied or recommended by the Supplier pursuant to this Agreement or for a purpose not reasonably to be inferred from the Services Description or the provisions of this Agreement;

"IT" information and communications technology;

"IT Environment" the Supplier System;

"Joint Controllers"	where two or more Controllers jointly determine the purposes and means of processing;
"Key Performance Indicator"	the key performance indicators set out in Table 1 of Part A of Annex 1 of Schedule 2.2 (*Performance Levels*);
"Key Personnel"	those persons appointed by the Supplier to fulfil the Key Roles, being the persons listed in Schedule 9.2 (*Key Personnel*) against each Key Role as at the Effective Date or as amended from time to time in accordance with Clauses 14.5 and 14.6 (*Key Personnel*);
"Key Roles"	a role described as a Key Role in Schedule 9.2 (*Key Personnel*) and any additional roles added from time to time in accordance with Clause 14.4 (*Key Personnel*);
"Key Sub-contract"	each Sub-contract with a Key Sub-contractor;
"Key Sub-contractor"	any Sub-contractor: (a) which, in the opinion of the Authority, performs (or would perform if appointed) a critical role in the provision of all or any part of the Services; and/or (b) with a Sub-contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the aggregate Charges forecast to be payable under this Agreement (as set out in the Pricing Model);
"Know-How"	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know how relating to the Services but excluding know how already in the other Party's possession before this Agreement;
"KPI Failure"	a failure to meet the Target Performance Level in respect of a Key Performance Indicator;
"KPI Service Threshold"	shall be as set out against the relevant Key Performance Indicator in Table 1 of Part A of Annex 1 of Schedule 2.2 (*Performance Levels*);
"Law"	any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, right within the meaning of Section 4(1) EU Withdrawal Act 2018 as amended by EU (Withdrawal

	Agreement) Act 2020 , regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply;
"Licensed Software"	all and any Software licensed by or through the Supplier, its Sub-contractors or any third party to the Authority for the purposes of or pursuant to this Agreement, including any Supplier Software and any Third Party Software;
"Losses"	losses, liabilities, damages, costs and expenses (including legal fees on a solicitor/client basis) and disbursements and costs of investigation, litigation, settlement, judgment interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty or otherwise;
"Maintenance Schedule"	shall have the meaning set out in Clause 9.4 (*Maintenance*);
"Malicious Software"	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
"Management Information"	the management information specified in Schedule 2.2 (*Performance Levels*), Schedule 7 (*Charges and Invoicing*) and Schedule 8 (*Governance*) to be provided by the Supplier to the Authority;
"Minor KPI Failure"	shall be as set out against the relevant Key Performance Indicator in Table 1 of Part A of Annex 1 of Schedule 2.2 (*Performance Levels*);
"month"	a calendar month and "**monthly**" shall be interpreted accordingly;
"Multi-Party Dispute Resolution Procedure"	has the meaning given in Paragraph 9.1 of Schedule 8.3 (*Dispute Resolution Procedure*);
"Multi-Party Procedure Initiation Notice"	has the meaning given in Paragraph 9.2 of Schedule 8.3 (*Dispute Resolution Procedure*);

"NCSC"	the National Cyber Security Centre or any replacement or successor body carrying out the same function;
"New Releases"	an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;
"Non-trivial Customer Base"	a significant customer base with respect to the date of first release and the relevant market but excluding Affiliates and other entities related to the licensor;
"Notifiable Default"	shall have the meaning given in Clause 28.1 (*Rectification Plan Process*);
"Object Code"	software and/or data in machine-readable, compiled object code form;
"Occasion of Tax Non-Compliance"	(a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 is found on or after 1 April 2013 to be incorrect as a result of: (i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle; (ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime; and/or (b) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 gives rise on or after 1 April 2013 to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Effective Date or to a civil penalty for fraud or evasion;
"Open Book Data"	has the meaning given in Schedule 7.5 (*Financial Reports and Audit Rights*);

"Open Source"	computer Software that is released on the internet for use by any person, such release usually being made under a recognised open source licence and stating that it is released as open source;
"Operating Environment"	the Sites;
"Operational Change"	any change in the Supplier's operational procedures which in all respects, when implemented: (a) will not affect the Charges and will not result in any other costs to the Authority; (b) may change the way in which the Services are delivered but will not adversely affect the output of the Services or increase the risks in performing or receiving the Services; (c) will not adversely affect the interfaces or interoperability of the Services with any of the Authority's IT infrastructure; and (d) will not require a change to this Agreement;
"Service Commencement Date"	1 April 2022;
"Other Supplier"	any supplier to the Authority (other than the Supplier) which is notified to the Supplier from time to time and/or of which the Supplier should have been aware;
"Parent Undertaking"	has the meaning set out in section 1162 of the Companies Act 2006;
"Partial Termination"	the partial termination of this Agreement to the extent that it relates to the provision of any part of the Services as further provided for in Clause 34.2(b) (*Termination by the Authority*) or 34.3(b) (*Termination by the Supplier*) or otherwise by mutual agreement by the Parties;
"Parties" and **"Party"**	have the meanings respectively given on page 1 of this Agreement;
"Performance Failure"	a KPI Failure;
"Performance Indicators"	the Key Performance Indicators;

"Permitted Maintenance"	has the meaning given in Clause 9.4 (*Maintenance*);
"Performance Monitoring Report"	has the meaning given in Schedule 2.2 (*Performance Levels*);
"Personal Data"	has the meaning given in the UK GDPR;
"Personal Data Breach"	has the meaning given in the UK GDPR;
"Preceding Services"	has the meaning given in Clause 5.2(b) (*Standard of Services*);
"Pricing Model"	the model setting out the Charges for the Services as set out in Schedule 7.1;
"Processor"	has the meaning given to it under the UK GDPR;
"Processor Personnel"	means all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Agreement;
"Prohibited Act"	(a) to directly or indirectly offer, promise or give any person working for or engaged by the Authority a financial or other advantage to: (i) induce that person to perform improperly a relevant function or activity; or (ii) reward that person for improper performance of a relevant function or activity; (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 this Agreement; (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 the Authority (including

offences by the Supplier under Part 3 of the Criminal Finances Act 2017); or

(d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK;

"Protective Measures" appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it;

"Project Specific IPRs"

(a) Intellectual Property Rights in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Agreement and updates and amendments of these items including (but not limited to) database schema; and/or

(b) Intellectual Property Rights arising as a result of the performance of the Supplier's obligations under this Agreement;

but shall not include the Supplier Background IPRs;

"Public Sector Dependent Supplier" means a supplier where that supplier, or that supplier's group has Annual Revenue of [redacted] million or more of which over 50% is generated from UK Public Sector Business;

"Public Sector and CNI Contract Information" means the information requirements set out in accordance with Paragraphs 11 to 13 and Annex 2 of Part B of Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);

"Publishable Performance Information" means any of the information in the Performance Monitoring Report as it relates to a Performance Indicator where it is expressed as publishable in the table in Annex 1 which shall not constitute Commercially Sensitive Information;

"Quality Plans" has the meaning given in Clause 6.1 (*Quality Plans*);

"Quarter" the first three Service Periods and each subsequent three Service Periods (save that the final Quarter shall

	end on the date of termination or expiry of this Agreement);
"Recipient"	has the meaning given in Clause 22.1 (*Confidentiality*);
"Records"	has the meaning given in Schedule 8.4 (*Reports and Records Provisions*);
"Rectification Plan"	a plan to address the impact of, and prevent the reoccurrence of, a Notifiable Default;
"Rectification Plan Failure"	(a) the Supplier failing to submit or resubmit a draft Rectification Plan to the Authority within the timescales specified in Clauses 28.4 (*Submission of the draft Rectification Plan*) or 28.8 (*Agreement of the Rectification Plan*); (b) the Authority, acting reasonably, rejecting a revised draft of the Rectification Plan submitted by the Supplier pursuant to Clause 28.7 (*Agreement of the Rectification Plan*); (c) the Supplier failing to rectify a material Default within the later of: (i) 30 Working Days of a notification made pursuant to Clause 28.2 (*Notification*); and (ii) where the Parties have agreed a Rectification Plan in respect of that material Default and the Supplier can demonstrate that it is implementing the Rectification Plan in good faith, the date specified in the Rectification Plan by which the Supplier must rectify the material Default; (d) following the successful implementation of a Rectification Plan, the same Notifiable Default recurring within a period of 6 months for the same (or substantially the same) root cause as that of the original Notifiable Default;
"Rectification Plan Process"	the process set out in Clauses 28.4 (*Submission of the draft Rectification Plan*) to 28.9 (*Agreement of the Rectification Plan*);
"Registers"	has the meaning given in Schedule 8.5 (*Exit Management*);

"Relevant Authority" or "Relevant Authorities"	means the Authority and the Cabinet Office Markets and Suppliers Team or, where the Supplier is a Strategic Supplier, the Cabinet Office Markets and Suppliers Team;
"Relevant IPRs"	IPRs used to provide the Services or as otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Authority or a third party in the fulfilment of the Supplier's obligations under this Agreement including IPRs in the Supplier Non-COTS Software, the Supplier Non-COTS Background IPRs, the Third Party Non-COTS Software and the Third Party Non-COTS IPRs but excluding any IPRs in the Authority Background IPRs, the Supplier COTS Software, the Supplier COTS Background IPRS, the Third Party COTS Software and/or the Third Party COTS IPRs;
"Relevant Preceding Services"	has the meaning given in Clause 5.2(b) (*Standard of Services*);
"Relevant Requirements"	all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State for Justice pursuant to section 9 of the Bribery Act 2010;
"Relevant Tax Authority"	HMRC, or, if applicable, a tax authority in the jurisdiction in which the Supplier is established;
"Relevant Transfer"	a transfer of employment to which the Employment Regulations applies;
"Relief Notice"	has the meaning given in Clause 32.2 (*Authority Cause*);
"Remedial Adviser"	the person appointed pursuant to Clause 30.2 (*Remedial Adviser*);
"Remedial Adviser Failure"	has the meaning given in Clause 30.6 (*Remedial Adviser*);
"Replacement Services"	any services which are the same as or substantially similar to any of the Services and which the Authority receives in substitution for any of the Services following the expiry or termination or Partial Termination of this Agreement, whether those services are provided by the Authority internally and/or by any third party;

"Replacement Supplier"	any third party service provider of Replacement Services appointed by the Authority from time to time (or where the Authority is providing replacement Services for its own account, the Authority);
"Request For Information"	a Request for Information under the FOIA or the EIRs;
"Required Action"	has the meaning given in Clause 31.1(a) (*Step-In Rights*);
"Retained Deliverables"	has the meaning given in Clause 35.8(b) (*Payments by the Supplier*);
"Risk Register"	the register of risks and contingencies that have been factored into any Costs due under this Agreement as set out in Annex 4 of Schedule 7 (*Charges and Invoicing*);
"Security Management Plan"	the Supplier's security plan as attached as Annex 2 of Schedule 2.4 (*Security Management*) and as subsequently developed and revised pursuant to Paragraphs 3 and 4 of Schedule 2.4 (*Security Management*);
"Serious KPI Failure"	shall be as set out against the relevant Key Performance Indicator in Table 1 of Part A of Annex 1 of Schedule 2.2 (*Performance Levels*);
"Service Charges"	the periodic payments made in accordance with Schedule 7 (*Charges and Invoicing*) in respect of the supply of the Services;
"Service Continuity Plan"	any plan prepared pursuant to Paragraph 2 of Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*) as may be amended from time to time;
"Service Continuity Services"	the business continuity, disaster recovery and insolvency continuity services set out in Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);
"Service Credit Cap"	the maximum level of Service Credits that may be deducted under Part C of Schedule 7.1 (Charges and Invoicing) which equates to [redacted];
"Service Credits"	credits payable by the Supplier due to the occurrence of 1 or more KPI Failures, calculated in accordance

	with Paragraph 1 of Part C of Schedule 7.1 (*Charges and Invoicing*);
"Service Period"	a calendar month, save that: (a) the first service period shall begin on the Service Commencement Date and shall expire at the end of the calendar month in which the Service Commencement Date falls; and (b) the final service period shall commence on the first day of the calendar month in which the Term expires or terminates and shall end on the expiry or termination of the Term;
"Service Points"	in relation to a KPI Failure, the points that are set out against the relevant Key Performance Indicator in the fifth column of the table in Annex 1 of Schedule 2.2 (*Performance Levels*);
"Services"	any and all of the services to be provided by the Supplier under this Agreement, including those set out in Schedule 2 (*Services Description*);
"Service Transfer Date"	has the meaning given in Schedule 9 (*Staff Transfer*);
"Services Description"	the services description set out in Schedule 2 (*Services Description*);
"Severe KPI Failure"	shall be as set out against the relevant Key Performance Indicator in Table 1 of Part A of Annex 1 of Schedule 2.2 (*Performance Levels*);
"Sites"	any premises (including, the Supplier's premises or third party premises): (a) from, to or at which: (i) the Services are (or are to be) provided; or (ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or (b) where: (i) any part of the Supplier System is situated;
"SME"	an enterprise falling within the category of micro, small and medium-sized enterprises defined by the

	Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises;
"Social Value"	the social, economic or environmental benefits set out in the Authority's Requirements;
"Software"	Supplier Software and Third Party Software;
"Software Supporting Materials"	has the meaning given in Clause 17.1(b) (*Project Specific IPRs*);
"Source Code"	computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;
"Specific Change in Law"	a Change in Law that relates specifically to the business of the Authority and which would not affect a Comparable Supply;
"Staffing Information"	has the meaning given in Schedule 9 (*Staff Transfer*);
"Standards"	the standards, polices and/or procedures identified in Schedule 2.3 (*Standards*);
"Step-In Notice"	has the meaning given in Clause 31.1 (*Step-In Rights*);
"Step-In Trigger Event"	(a) any event falling within the definition of a Supplier Termination Event; (b) a Default by the Supplier that is materially preventing or materially delaying the performance of the Services or any material part of the Services; (c) the Authority considers that the circumstances constitute an emergency despite the Supplier not being in breach of its obligations under this Agreement; (d) the Authority being advised by a regulatory body that the exercise by the Authority of its rights under Clause 31 (*Step-In Rights*) is necessary;

	(e) the existence of a serious risk to the health or safety of persons, property or the environment in connection with the Services; and/or (f) a need by the Authority to take action to discharge a statutory duty;
"Step-Out Date"	has the meaning given in Clause 31.5(b) (*Step-In Rights*);
"Step-Out Notice"	has the meaning given in Clause 31.5 (*Step-In Rights*);
"Step-Out Plan"	has the meaning given in Clause 31.6 (*Step-In Rights*);
"Strategic Supplier"	means those suppliers to government listed at https://www.gov.uk/government/publications/strategic-suppliers;
"Sub-contract"	any contract or agreement (or proposed contract or agreement) between the Supplier (or a Sub-contractor) and any third party whereby that third party agrees to provide to the Supplier (or the Sub-contractor) all or any part of the Services or facilities or services which are material for the provision of the Services or any part thereof or necessary for the management, direction or control of the Services or any part thereof;
"Sub-contractor"	any third party with whom: (a) the Supplier enters into a Sub-contract; or (b) a third party under (a) above enters into a Sub-contract, or the servants or agents of that third party;
"Sub-processor"	any third party appointed to process Personal Data on behalf of the Supplier related to this Agreement;
"Subsidiary Undertaking"	has the meaning set out in section 1162 of the Companies Act 2006;
"Successor Body"	has the meaning given in Clause 37.4 (*Assignment and Novation*);
"Supplier Background IPRs"	(a) Intellectual Property Rights owned by the Supplier before the Effective Date, for example those subsisting in the Supplier's standard development tools, program components or standard code used in computer programming or in physical or

	electronic media containing the Supplier's Know-How or generic business methodologies; and/or (b) Intellectual Property Rights created by the Supplier independently of this Agreement, which in each case is or will be used before or during the Term for designing, testing implementing or providing the Services but excluding Intellectual Property Rights owned by the Supplier subsisting in the Supplier Software;
"Supplier COTS Background IPRs"	Any embodiments of Supplier Background IPRs that: (a) the Supplier makes generally available commercially prior to the date of this Agreement (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price; and (b) has a Non-trivial Customer Base;
"Supplier COTS Software"	Supplier Software (including open source software) that: (a) the Supplier makes generally available commercially prior to the date of this Agreement (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the Supplier save as to price; and (b) has a Non-trivial Customer Base;
"Supplier Equipment"	the hardware, computer and telecoms devices and equipment used by the Supplier or its Sub-contractors (but not hired, leased or loaned from the Authority) for the provision of the Services;
"Supplier Group"	means the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings;
"Supplier Non-COTS Background IPRs"	Any embodiments of Supplier Background IPRs that have been delivered by the Supplier to the Authority and that are not Supplier COTS Background IPRs;
"Supplier Non-COTS Software"	Supplier Software that is not Supplier COTS Software;

"Supplier Non-Performance"	has the meaning given in Clause 32.1 (*Authority Cause*);
"Supplier Personnel"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Sub-contractor engaged in the performance of the Supplier's obligations under this Agreement;
"Supplier Representative"	the representative appointed by the Supplier pursuant to Clause 11.3 (*Representatives*);
"Supplier Software"	software which is proprietary to the Supplier (or an Affiliate of the Supplier) and which is or will be used by the Supplier for the purposes of providing the Services, including the software specified as such in Schedule 5 (*Software*);
"Supplier Solution"	the Supplier's solution for the Services set out in Schedule 4 (*Supplier Solution*) including any Annexes of that Schedule;
"Supplier System"	the information and communications technology system used by the Supplier in implementing and performing the Services including the Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Authority System);
"Supplier Termination Event"	(a) the Supplier committing a material Default which is irremediable; (b) as a result of the Supplier's Default, the Authority incurring Losses in any Contract Year which exceed 80% of the value of the aggregate annual liability cap for that Contract Year as set out in Clause 26.6(a) (*Financial and other Limits*); (c) a Remedial Adviser Failure; (d) a Rectification Plan Failure; (e) where a right of termination is expressly reserved in this Agreement, including pursuant to: (i) Clause 19 (*IPRs Indemnity*); (ii) Clause 40.6(b) (*Prevention of Fraud and Bribery*); and/or

(iii) Paragraph 6 of Schedule 7.4 (*Financial Distress*);

(iv) Paragraph 12 of Part B to Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);

(f) the representation and warranty given by the Supplier pursuant to Clause 3.2(i) (*Warranties*) being materially untrue or misleading;

(g) the Supplier committing a material Default under Clause 10.10 (*Promoting Tax Compliance*) or failing to provide details of steps being taken and mitigating factors pursuant to Clause 10.10 (*Promoting Tax Compliance*) which in the reasonable opinion of the Authority are acceptable;

(h) the Supplier committing a material Default under any of the following Clauses:

(i) Clause 5.5(j) (*Services*);

(ii) Clause 24 (*Protection of Personal Data*);

(iii) Clause 23 (*Transparency and Freedom of Information*);

(iv) Clause 22 (*Confidentiality*); and

(v) Clause 36 (*Compliance*); and/or

(vi) in respect of any security requirements set out in Schedule 2 (*Services Description*), Schedule 2.4 (*Security Management*) or the Security Requirements; and/or

(vii) in respect of any requirements set out in Schedule 9 (*Staff Transfer*);

(i) an Insolvency Event occurring in respect of the Supplier;

(j) a change of Control of the Supplier unless:

(i) the Authority has given its prior written consent to the particular Change of Control, which subsequently takes place as proposed; or

(ii) the Authority has not served its notice of objection within 6 months of the later of the date on which the Change of Control took

place or the date on which the Authority was given notice of the Change of Control;

(k) a change of Control of a Key Sub-contractor unless, within 6 months of being notified by the Authority that it objects to such change of Control, the Supplier terminates the relevant Key Sub-contract and replaces it with a comparable Key Sub-contract which is approved by the Authority pursuant to Clause 15.10 (*Appointment of Key Sub-contractors*);

(l) the Authority has become aware that the Supplier should have been excluded under Regulation 57(1) or (2) of the Public Contracts Regulations 2015 from the procurement procedure leading to the award of this Agreement;

(m) a failure by the Supplier to comply in the performance of the Services with legal obligations in the fields of environmental, social or labour law; or

(n) in relation to Schedule 2.4 (*Security Requirements*):

(i) the Authority has issued two rejection notices in respect of the Security Management Plan under Paragraph 4.5(b) (Part A);

(ii) the Supplier fails to implement a change required by the Required Changes Register in accordance with the timescales set out in the Required Changes Register;

(iii) Supplier COTS Software and Third Party COTS Software is not within mainstream support unless the Authority has agreed in writing.

(iv) the Supplier fails to patch vulnerabilities in accordance with the Security Requirements; and/or,

(v) the Supplier fails to comply with the Incident Management Process.

"Supply Chain Transparency Report" means the report provided by the Supplier to the Authority in the form set out in Annex 3 of Schedule 8.4 (*Reports and Records Provisions*);

"Target Performance Level"	the minimum level of performance for a Performance Indicator which is required by the Authority, as set out against the relevant Performance Indicator in the tables in Annex 1 of Schedule 2.2 (*Performance Levels*);
"Term"	the period commencing on the 1 April 2022 (being the Service Commencement Date) and ending on 31 August 2023 or on earlier termination of this Agreement;
"Termination Assistance Notice"	has the meaning given in Paragraph 5 of Schedule 8.5 (*Exit Management*);
"Termination Assistance Period"	in relation to a Termination Assistance Notice, the period specified in the Termination Assistance Notice for which the Supplier is required to provide the Termination Services as such period may be extended pursuant to Paragraph 5.2 of Schedule 8.5 (*Exit Management*);
"Termination Date"	the date set out in a Termination Notice on which this Agreement (or a part of it as the case may be) is to terminate;
"Termination Notice"	a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate this Agreement (or any part thereof) on a specified date and setting out the grounds for termination;
"Termination Payment"	the payment determined in accordance with Schedule 7.2 (*Payments on Termination*);
"Termination Services"	the services and activities to be performed by the Supplier pursuant to the Exit Plan, including those activities listed in Annex 1 of Schedule 8.5 (*Exit Management*), and any other services required pursuant to the Termination Assistance Notice;
"Third Party Auditor"	an independent third party auditor as appointed by the Authority from time to time to confirm the completeness and accuracy of information uploaded to the Virtual Library in accordance with the requirements outlined in Schedule 8.4 (*Reports and Records Provisions*);
"Third Party Beneficiary"	has the meaning given in Clause 44.1 (*Third Party Rights*);

"Third Party COTS IPRs"	Third Party IPRs that: (a) the supplier makes generally available commercially prior to the date of this Agreement (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the supplier save as to price; and (b) has a Non-trivial Customer Base;
"Third Party COTS Software"	Third Party Software (including open source software) that: (a) the supplier makes generally available commercially prior to the date of this Agreement (whether by way of sale, lease or licence) on standard terms which are not typically negotiated by the supplier save as to price; and (b) has a Non-trivial Customer base;
"Third Party IPRs"	Intellectual Property Rights owned by a third party but excluding Intellectual Property Rights owned by the third party subsisting in any Third Party Software;
"Third Party Non-COTS IPRs"	Third Party IPRs that are not Third Party COTS IPRs;
"Third Party Non-COTS Software"	Third Party Software that is not Third Party COTS Software;
"Third Party Provisions"	has the meaning given in Clause 44.1 (*Third Party Rights*);
"Third Party Software"	software which is proprietary to any third party (other than an Affiliate of the Supplier) or any Open Source Software which in any case is, will be or is proposed to be used by the Supplier for the purposes of providing the Services, including the software specified as such in Schedule 5 (*Software*);
"Transferring Assets"	has the meaning given in Paragraph 6.2(a) of Schedule 8.5 (*Exit Management*);
"Transferring Authority Employees"	has the meaning given in Schedule 9 (*Staff Transfer*);
"Transferring Former Supplier Employees"	has the meaning given in Schedule 9 (*Staff Transfer*);

"Transferring Supplier Employees"	has the meaning given in Schedule 9 (*Staff Transfer*);
"Transparency Information"	has the meaning given in Clause 23.1 (*Transparency and Freedom of Information*);
"Transparency Reports"	has the meaning given in Schedule 8.4 (*Reports and Records Provisions*);
"UK"	the United Kingdom;
"UK Public Sector Business"	means any goods, service or works provision to UK public sector bodies, including Central Government Departments and their arm's length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police, fire and rescue, education bodies and devolved administrations;
"UK Public Sector / CNI Contract Information"	means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 11 to 13 and Annex 2 of Part B of Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);
UK GDPR	the General Data Protection Regulation (Regulation (EU) 2016/679) as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018, together with the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019;
"Unconnected Sub-contract"	any contract or agreement which is not a Sub-contract and is between the Supplier and a third party (which is not an Affiliate of the Supplier) and is a qualifying contract under regulation 6 of The Reporting on Payment Practices and Performance Regulations 2017;
"Unconnected Sub-contractor"	any third party with whom the Supplier enters into an Unconnected Sub-contract;
"Unrecovered Payment"	has the meaning given in Schedule 7.2 (*Payments on Termination*);
"Updates"	in relation to any Software and/or any Deliverable means a version of such item which has been

	produced primarily to overcome Defects in, or to improve the operation of, that item;
"Upgrades"	any patch, New Release or upgrade of Software and/or a Deliverable, including standard upgrades, product enhancements, and any modifications, but excluding any Update which the Supplier or a third party software supplier (or any Affiliate of the Supplier or any third party) releases during the Term;
"Valid"	in respect of an Assurance, has the meaning given to it in Paragraph 11.7 of Part B to Schedule 8.6 (*Service Continuity Plan and Corporate Resolution Planning*);
"VAT"	value added tax as provided for in the Value Added Tax Act 1994;
"VCSE"	means a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives;
"Working Day"	any day other than a Saturday, Sunday or public holiday in England and Wales.

MODEL AGREEMENT FOR SERVICES SCHEDULES

SCHEDULE 2

SCHEDULE 2.1

SERVICES DESCRIPTION

Services Description

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

"Programme" means the Science CPD Programme

2 INTRODUCTION AND BACKGROUND

2.1 This Schedule sets out the intended scope of the Services to be provided by the Supplier to deliver the Programme and to provide a description of what the Services entail.

2.2 The government has stated a clear ambition for the UK to cement its place as a 'science superpower'. The UK is therefore expected to a see an increase in jobs requiring STEM skills, which will be an important contributor to economic growth. This means that a secure and sufficient pipeline of pupils studying science subjects and performing well in them is needed. This pipeline begins with the provision of regular, high quality science lessons to drive performance at primary level, and continues through to key stage 4 and 5, where the challenge is also to drive uptake and bolster exam performance.

2.3 Overall, A level exam entries in the sciences have increased significantly over the past decade, as have the number of students completing the EBacc science component. The challenge is not only to sustain this overall progress by supporting each stage of science education, but also to address the particular issues that science education faces. These are:

- The need to drive good outcomes for all and at all levels, especially following the impact of Covid-19 on learning, and in particular to address the disadvantage gap in performance at GCSE and A level.
- The need to continue driving participation in A level sciences, and in particular to pursue measures to tackle the longstanding low levels of uptake of A level physics, particularly by females.
- The need to bolster the confidence of primary science teachers in delivering all aspects of the primary national curriculum for science.
- The need to encourage science teacher retention (particularly physics teacher retention) in the context of high levels of turnover.

2.4 Supporting good quality teaching is paramount for addressing these challenges - both in terms of supporting effective delivery of lessons and subsequent outcomes and also for inspiring students to continue studying science subjects to a higher level. The department has committed to level up education standards across the country so that children and young people in every part of the country are prepared with the knowledge, skills and qualifications they need. This includes addressing the disadvantage gap in performance.

2.5 The overall aim of the Programme is, therefore, to deliver CPD to support teachers and raise the quality of teaching to help the delivery of brilliant lessons. This is expected to not only benefit pupil outcomes and participation, but also teacher confidence and retention in science subjects.

3 SERVICES DESCRIPTION

3.1 Services

3.1.1 The purpose of the Programme is to deliver CPD for the sciences to state-funded schools in order to raise the quality of science teaching and to support teachers. At primary level this shall cover the teaching of primary science as part of the national curriculum, and at secondary level shall cover the separate sciences of biology, chemistry and physics at key stage 3, GCSE and A level.

3.1.2 The Authority remains committed to the 2021-22 delivery model of bursary funding to provide targeted access to CPD and two separate school-led networks: Science Learning Partnerships, covering all three sciences and primary science, and the Stimulating Physics Network giving targeted support to physics teaching in order to improve the take-up of A level physics.

3.1.3 To simplify governance, administration and contractual and grant funding arrangements and promote financial efficiency and consistency of approach, the three programmes have been rolled into this Agreement comprising a single oversight and administration body.

3.1.4 The aim of the programmes shall continue to be to provide support to teachers in order to improve their teaching. This means providing CPD that helps develop subject pedagogy and subject knowledge, supports teachers to raise participation levels in science in their school, and helps teachers to become more confident practitioners. By aiding teacher development in these areas, the programmes should also support the aim of encouraging greater levels of teacher retention in the sciences.

3.1.5 The Supplier shall work quickly to build relationships with the existing lead schools in these networks, harness the value they hold and assess capacity and ensure the very best schools are engaged in the delivery of CPD for the duration of the Term .

3.1.6 The Supplier shall deliver the Services in accordance with the project plan set out in Schedule 4.1 (Supplier Solution).

3.2 Specific requirements

3.2.1 The Supplier shall design the CPD provided by the Programme in line with best practice in CPD design, underpinned by robust evidence and expertise. In particular, the CPD shall be designed with due regard to the principles outlined in the ‘designing effective

professional development' section of the Authority's NPQ in Leading Teacher Development guidance.

3.2.2 The CPD provided by the Programme shall support a knowledge-rich curriculum, developing both the substantive knowledge and disciplinary knowledge of teachers to give them a strong knowledge base for their teaching. It shall also develop teachers' pedagogical content knowledge and reflect the latest understanding of effective subject-specific pedagogy. This is especially important for teachers who are teaching outside their specialism, and the CPD shall give particular regard to these teachers.

3.2.3 In addition, the CPD shall support teachers and technicians to deliver safe, purposeful and effective practical work, including both teacher demonstrations and pupil practical work. Specifically, teachers shall be supported in understanding the role of practical work in supporting the delivery of a knowledge-rich curriculum. As with other CPD, this practical-oriented CPD shall focus on the learning benefits for pupils.

3.2.4 The Authority expects strategies to develop science capital to be embedded within the CPD delivered by the Programme. This means aiding teachers to develop strategies to support their students' personal contextualisation of science, with the aim of encouraging students to believe that 'science is for them' in order to drive uptake of science at higher levels and support all pupils to become scientifically literate citizens.

3.2.5 The Supplier shall work with a range of scientific and educational organisations (e.g. learned societies, awarding organisations, NCETM, teaching school hubs, Isaac Physics) to enhance the reach and impact of the CPD and networks and to avoid duplication of work.

3.2.6 During the Term, the Supplier shall demonstrate how funding for central administration of the programme will be used efficiently in a manner that maximises the money invested in CPD and impact of the Programme

3.3 In detail, the programme requirements are to:

<u>Science Learning Partnerships</u>

Key Objectives

3.3.1 The purpose of the SLP network is to improve the standards of science teaching in primary and secondary schools and FE colleges through improved subject knowledge and pedagogy

CPD design

3.3.2 The school-based network of Science Learning Partnerships (SLPs) shall provide CPD to teachers and technicians delivering primary

science and the separate sciences at key stage 3 through to A level. As well as providing an offer to all schools, the SLP network shall particularly encourage meaningful engagement from schools with the highest percentage of pupils eligible for the Pupil Premium.

3.3.3 At a primary level, focus shall be given to confidence in delivering a curriculum in primary science that places knowledge and learning at its core, rather than being activity-led. The Programme shall provide particular support to primary science leaders to allow them to disseminate this learning to colleagues in order to increase knowledge and confidence in teaching science in their schools.

3.3.4 At a secondary level, CPD shall be specific to biology, chemistry and physics. In particular, the Programme shall offer tailored support to those teachers who are teaching outside their specialism. There shall also be particular support for schools offering triple science, or looking to do so, to strengthen their provision.

3.3.5 The Programme will need to have the flexibility to deliver CPD according to evolving government priorities. In line with current government priorities, therefore, dedicated CPD shall be made available to support the teaching of climate change in line with the national curriculum.

Delivery model

3.3.6 The Supplier shall maintain the 2021-22 delivery model of the SLP programme and the SLP network and resources developed under the 2021-22 contract (as set out in the Asset Register) shall transition to the Supplier (subject to an audit of existing SLPs).

- Audit and ongoing monitoring of SLPs

3.3.7 The Supplier shall carry out a rapid audit of the network of SLPs at the start of the Term to assess capacity of each school to continue to operate as an SLP. The Supplier, as part of this audit, shall also implement an agreed procedure to terminate the status of an SLP where necessary and find a high-quality replacement SLP school as required. The Supplier will continue to monitor the performance of each SLP and apply a review process accordingly (setting out timescales for required improvement where necessary leading to the maintaining of an SLP status or removing it). Outputs of this process will be reported back to the Authority by the Supplier via monthly contract meetings and reports to provided in accordance with Schedule 8 (Governance).

- Network of SLPs

3.3.8 The Supplier shall be responsible for maintaining and coordinating a network of 25-30 SLPs ensuring there is good geographical coverage across England. This shall include responsibility for working with the Authority to set the strategic priorities and a

programme of delivery for the network that will provide, at a minimum 17500 days of CPD annually. The Supplier shall also have a responsibility to recruit, support and monitor SLPs and ensure that the network of SLPs collaborate effectively.

- CPD resources

3.3.9 The Supplier shall be responsible for developing and maintaining a bank of high-quality resources to be used in the delivery of science CPD and to make these accessible to SLPs. These resources will need to be aligned to annual strategic priorities agreed with DfE and identified local needs in schools. The Supplier shall also need to reflect the latest research and evidence on effective CPD and science-related curriculum topics.

- CPD delivery

3.3.10 The Supplier shall be responsible for supporting each SLP to provide a programme of subject-specific CPD and engage with a range and number of schools appropriate to ensuring national coverage of the strategic priorities. The Supplier shall ensure that delivery of CPD is of a consistent high-quality standard across the SLP network and that there is effective sharing of best practice between SLPs.

3.3.11 The Supplier shall work with each SLP to ensure that, based on the work of that SLP, it has access to a suitable number of appropriately qualified individuals to deliver CPD. Where appropriate, the Supplier shall provide those delivering CPD with such ongoing support and professional development as is necessary to ensure that they are able to serve effectively in their SLP.

3.3.12 The Supplier shall also have responsibility for ensuring that each SLP utilises different modes of delivery to ensure any service is accessible, available, performant and resilient and that each SLP has a business continuity plan, including a plan for adapting the delivery model to remote-only in response to circumstances such as tightening of Covid-19 restrictions.

3.3.13 The Supplier shall be responsible for the ongoing monitoring, refinement and evaluation of CPD, capturing and disseminating findings within the SLP network to ensure that they are able to inform future CPD. The Supplier shall also be required to cooperate with the Authority, and any external evaluator appointed by the Authority, with regards to evaluation of provision and its impact.

3.3.14 When developing and implementing digital or technology services, the Supplier shall work within guidelines set out in the Government's Service Standard and comply with Web Content Accessibility Guidelines (WCAG) 2.1 'AA' standard.

Funding arrangements

3.3.15 In maintaining the network, the Supplier shall be responsible for funding the SLPs and each academic year develop a SLP funding model, to be agreed with the Authority, assuming an affordable charge to schools receiving CPD.

Stimulating Physics Network

Key objectives

3.3.16 The purpose of the Stimulating Physics Network (SPN) is to provide tailored support through a network of lead schools to a cohort of partner schools to increase both the rates of progression to physics A level and the number of students from under-represented groups progressing to physics A level.

CPD design

3.3.17 The SPN shall provide intensive support to those partner schools that have low progression rates to A level physics and through this work the SPN shall help inspire more students to study A level physics. The SPN shall also offer more general support to all physics teachers, including early career teachers, in order to improve teacher retention rates in physics.

3.3.18 Within an overall increase in numbers, the SPN's work shall aim to narrow the gap in the proportion of boys and girls choosing to study physics at A level. It shall also look to increase the number of students eligible for free school meals choosing to study physics A level. To support this, SPN shall promote strategies with teachers that develop science capital in under-represented groups of pupils, giving regard to the latest research on what is effective in engendering a positive attitude to physics and a belief that 'physics is for them'.

3.3.19 The Supplier of the SPN shall give due regard to the work of other organisations that are also working to promote participation by underrepresented groups in physics, engineering and related areas and seek opportunities for collaboration where possible.

3.3.20 Alongside the core SPN, the Supplier shall manage and oversee the Subject Knowledge for Physics Teaching (SKPT) programme. The aim of SKPT is to increase the number of trained physics teachers in the teaching workforce through provision of high-quality training in particular areas of physics for teachers teaching physics at Key Stage 3 and/or Key Stage 4 outside of their specialist field.

3.3.21 The Supplier shall also provide management and oversight of the 'Inclusion in Schools programme' which aims to increase the number of students progressing to physics-based education at post-

16 from underrepresented groups. It does this through targeted interventions to address barriers to inclusion at a whole-school level.

Delivery model

3.3.22 As with the SLP programme, the Supplier shall maintain the 2021-22 delivery model of the SPN programme and the network of lead SPN schools and physics coaches and resources developed under the previous contract as detailed in the Asset Registers shall transition to the Supplier (subject to appropriate auditing of lead schools).

- Audit of existing lead schools

3.3.23 The Supplier shall carry out a rapid audit of the existing network of lead SPN schools and their physics coaches to quickly establish relationships with each and assess capacity to continue to operate as a lead SPN school. The Supplier will also implement an agreed procedure to terminate the status of an SPN lead school and apply the procedure where appropriate and find a high-quality replacement SPN lead school as required. The Supplier will continue to monitor the performance of each SLP and apply a review process accordingly (setting out timescales for required improvement where necessary leading to the maintaining of an SLP status or removing it). Outputs of this process will be reported back to the Authority by the Supplier via monthly contract meetings and reports to provided in accordance with Schedule 8 (Governance).

- The network of lead SPN schools

3.3.24 The Supplier shall be responsible for maintaining and coordinating a network of around 50 lead SPN schools, their physics coaches and partner schools (around 350) ensuring there is good geographical coverage across England. This will include responsibility for working with the Authority to set the strategic priorities and a programme of delivery for the network that will provide, at a minimum of 1,600 days of CPD annually. The Supplier shall also have a responsibility to recruit, support and monitor lead SPN schools and ensure that the network collaborates effectively.

- CPD resources

3.3.25 The Supplier shall be responsible for developing and maintaining a bank of high-quality resources to be used in the delivery of physics CPD and to make these accessible to lead SPN schools and their physics coaches. These resources will need to be aligned to annual strategic priorities agreed with the Authority and identified local needs in schools. The Supplier shall need to also reflect the latest research and evidence on effective CPD and science-related curriculum topics.

- CPD delivery

3.3.26 The Supplier shall be responsible for supporting each lead SPN school and their physics coach to provide a programme of physics CPD and engage with a range and number of partner schools to ensure national coverage of the strategic priorities. The Supplier shall ensure that delivery of CPD is of a consistent high-quality standard across the network and that there is effective sharing of best practice between lead SPN schools / physics coaches.

3.3.27 The Supplier shall work with each lead SPN school and their physics coach to ensure that, based on the work of that school, it has access to a suitable number of appropriately qualified individuals to deliver CPD. Where appropriate, the Supplier shall provide those delivering CPD with such ongoing support and professional development as is necessary to ensure that they are able to serve effectively in their role.

3.3.28 The Supplier shall also have responsibility for ensuring that each lead SPN school utilises different modes of delivery to ensure any service is accessible, available, performant and resilient and that each has a business continuity plan, including a plan for adapting the delivery model to remote-only in response to circumstances such as tightening of Covid-19 restrictions.

3.3.29 The Supplier shall be responsible for the ongoing monitoring, refinement and evaluation of CPD, capturing and disseminating findings within the SPN network to ensure that they are able to inform future CPD. The Supplier shall also be required to cooperate with the Authority, and any external evaluator appointed by the Authority, with regards to evaluation of provision and its impact.

3.3.30 When developing and implementing digital or technology services, the Supplier shall work within guidelines set out in the Government's Service Standard and comply with Web Content Accessibility Guidelines (WCAG) 2.1 'AA' standard.

- Subject Knowledge for Physics Teaching

3.3.31 Through the Stimulating Physics Network, the Supplier shall deliver and continue to develop the Subject Knowledge for Physics Teachers (SKPT) programme. The above requirements of CPD delivery will also apply to the delivery of SKPT.

3.3.32 In addition, the Supplier shall be responsible for working annually with the Authority to develop and agree strategic priorities for the SKPT programme and an effective programme of delivery by a subset of SPN lead schools. The programme will deliver annually a minimum of 600 certified and assessed course modules covering the national curriculum physics topics to teachers teaching physics Key Stage 3 and/or Key Stage 4 outside of their specialist field. This includes managing the transition of teachers currently taking part in

the programme so that they are able to complete further modules under the new contract. The title for each SKPT course module is to be agreed with the Authority but expected to include pre-exiting SKPT course modules as well as additional new modules.

3.3.33 The Supplier shall be responsible for maintaining and coordinating a cohort of lead SPN schools sufficient to deliver the programme and provide a good geographical coverage of England. The Supplier shall have a responsibility to recruit, support and monitor this cohort of lead SPN schools delivering SKPT and ensure that they collaborate effectively and delivery of SKPT is of a consistent standard across the network.

3.3.34 The Supplier shall develop and maintain a bank of high-quality resources to be used in the delivery of CPD to support subject knowledge for non-specialist physics teachers and make these accessible to those lead SPN schools delivering SKPT.

- Inclusion in Schools programme

3.3.35 Through the Stimulating Physics Network, deliver and continue to develop the Inclusion in Schools programme. The above requirements of CPD delivery shall also apply to the delivery of the Inclusion in Schools programme.

3.3.36 In addition, the Supplier shall be responsible for recruiting and supporting a cohort of schools to participate in the Inclusion in Schools programme. The Supplier shall be responsible for ensuring around 100 schools are recruited to the programme and working with those schools with the aim of sustaining their participation in the programme.

3.3.37 The Supplier shall be responsible for recruiting and maintaining a team of Inclusion in Schools coaches so that each participating school is supported by a dedicated coach who will support them in the development and implementation of school specific action plans and provision of supporting resources aimed at increasing participation in post-16 physics by under-represented groups through a whole school approach to inclusion.

Funding arrangements

3.3.38 In maintaining the network, the Supplier shall be responsible for funding the lead SPN schools, including funding for the release of a school-based physics coach in each lead school, as well as for delivery of SKPT by a cohort of lead SPN schools and delivery of the Inclusion in Schools programme. The Supplier shall be responsible for developing a funding model, to be agreed with the Authority, assuming there is no charge to schools receiving CPD, including SKPT and the Inclusion in Schools programme. Funding for participants of the SKPT programme will be via bursaries which shall be administered by the Supplier.

Bursary scheme for CPD

3.3.39 The Supplier shall be responsible for overseeing the award and administration of a bursary scheme for CPD. The purpose of the bursary scheme is to allow access to high quality CPD with the aim of improving teacher subject knowledge and raising the quality of teaching in order to support the delivery of a knowledge-rich curriculum. The bursaries should be used to contribute to the cost of face-to-face CPD covering primary science and biology, chemistry and physics at key stage 3, GCSE and A level. The bursaries are to contribute to the cost of course fees, travel and subsistence and supply cover.

3.3.40 The bursaries are to be made available to a select group of state schools and colleges in England that meet a set of criteria agreed with by the department. The criteria should give consideration to the following groups:

- (Primary) All leaders of primary science. Courses are targeted towards those without a post-16 qualification in science. (Ofsted's Research Review in Science shows that just 5% of primary school teachers hold specialised science degrees and teaching qualifications in science).
- (Secondary) Areas of disadvantaged measured as LADs 5/6, Education Investment Areas and North-East Schools
- (Secondary) Pupil premium funding levels
- (Post-16 institutions) Areas of disadvantaged measured as LAD's 5/6, Education Investment Areas and North-East Schools
- LADs that have the lowest % of children attending good/outstanding schools
- Pupil premium funding levels
- Ofsted Inadequate

Delivery model

3.3.41 The Supplier shall be responsible for developing and delivering an effective programme of bursary awards for each academic year, to be agreed with the Authority and reflecting the above outline of the scheme and any additional strategic direction the Authority provides. The Supplier shall be responsible for ensuring that the bursary scheme supports teachers and support staff to access, at a minimum, 5,000 CPD days per year.

Funding arrangements

3.3.42 Each academic year, the Supplier shall develop a bursary funding model reflecting the above outline of the scheme and any additional strategic direction the Authority provides and to be maintained by the Supplier and agreed with the Authority.

Reporting

3.3.43 The Supplier shall hold monthly review meetings with the Authority (and more frequently if required) to monitor and report on programme performance against the Key Performance Indicators as detailed in Schedule 2.2 (Performance Levels) and agree with the Authority appropriate remedial action where this is required to address any areas of concern identified by the Supplier or the Authority.

3.4 Security Requirements

3.4.1 The Supplier shall comply with its obligations set out in Schedule 2.2 (Security Management) and the requirements set out in the National Cyber Security Centre (NCSC) guidelines.

MODEL AGREEMENT FOR SERVICES SCHEDULES

SCHEDULE 2.2

PERFORMANCE LEVELS

Performance Levels

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

"Service Period"	means each calendar month during the Term, save that: (a) the first service period shall begin on the Service Commencement Date and shall expire at the end of the calendar month in which the Service Commencement Date falls; and (b) the final service period shall commence on the first day of the calendar month in which the Term expires or terminates and shall end on the expiry or termination of the Term (the "Final Service Period");
"Performance Monitoring Report"	has the meaning given in Paragraph 1.1(a) of Part B;
"Performance Review Meeting"	the regular meetings between the Supplier and the Authority to manage and review the Supplier's performance under this Agreement, as further described in Paragraph 1.7 of Part B;

PART A: PERFORMANCE INDICATORS AND SERVICE CREDITS

1 PERFORMANCE INDICATORS

1.1 Annex 1 sets out the Key Performance Indicators which the Parties have agreed shall be used to measure the performance of the Services by the Supplier.

1.2 The Supplier shall monitor its performance against each Performance Indicator and shall send the Authority a report detailing the level of service actually achieved in accordance with Part B.

1.3 Service Points, and therefore Service Credits, shall accrue for any KPI Failure and shall be calculated in accordance with Paragraphs 2 and 5.

2 SERVICE POINTS

2.1 If the level of performance of the Supplier over the Term achieves the Target Performance Level in respect of a Key Performance Indicator, no Service Points shall accrue to the Supplier in respect of that Key Performance Indicator.

2.2 If the level of performance of the Supplier over the Term is below the Target Performance Level in respect of a Key Performance Indicator, Service Points shall accrue to the Supplier in respect of that Key Performance Indicator as set out in Paragraph 2.3.

2.3 The number of Service Points that shall accrue to the Supplier in respect of a KPI Failure shall be the applicable number as set out in Annex 1 depending on whether the KPI Failure is a Minor KPI Failure, a Serious KPI Failure, a Severe KPI Failure or is a failure by the Supplier to meet a KPI Service Threshold.

3 NOT USED

4 NOT USED

5 SERVICE CREDITS

5.1 Schedule 7 (*Charges and Invoicing*) sets out the mechanism by which Service Points shall be converted into Service Credits.

5.2 The Authority shall use the Final Performance Monitoring Report provided pursuant to Part B to verify the calculation and accuracy of the Service Credits (if any) applicable at the end of the Term.

5.3 For the avoidance of doubt, Service Credits shall only be applied to the co-ordinating body funding element of the Annual Service Charges as detailed in the Pricing Model.

PART B: PERFORMANCE MONITORING

1 PERFORMANCE MONITORING AND PERFORMANCE REVIEW

1.1 Within 10 Working Days of the end of each Service Period during the Term, the Supplier shall provide:

(a) a report to the Authority Representative which summarises the performance by the Supplier against each of the Performance Indicators as more particularly described in Paragraph 1.4 (the "**Performance Monitoring Report**"); and

(b) a report created by the Supplier to the Authority's senior responsible officer which summarises the Supplier's performance over the relevant Service Period as more particularly described in Paragraph 1.5 (the "**Balanced Scorecard Report**").

1.2 Within 10 Working Days following the end of the Term, the Supplier shall provide a report to the Authority Representative which summarises the performance by the Supplier against each of the Performance Indicators as more particularly described in Paragraph 1.8 (the " **Final Performance Monitoring Report**") over the Term.

1.3 Within 10 Working Days following the end of the Term, the Supplier shall provide a report to the Authority's senior responsible officer which summarises the Supplier's performance over the Term as more particularly described in Paragraph 1.10 (the "**Final Balanced Scorecard Report**").

Performance Monitoring Report

1.4 The Performance Monitoring Report shall be in such format as agreed between the Parties from time to time and contain, as a minimum, the following information:

Information in respect of the Service Period just ended

(a) for each Key Performance Indicator, the performance achieved over the Service Period and that achieved over the previous 3 Service Periods;

(b) the conduct and performance of any agreed periodic tests that have occurred, such as the annual failover test of the Service Continuity Plan;

(c) relevant particulars of any aspects of the Supplier's performance which fail to meet the requirements of this Agreement; and

(d) such other details as the Authority may reasonably require from time to time;

Information in respect of previous Service Periods

(a) the conduct and performance of any agreed periodic tests that have occurred in such Service Period such as the annual failover test of the Service Continuity Plan;

Balanced Scorecard Report

1.5 The Balanced Scorecard Report shall be presented in the form of an accessible dashboard and, as a minimum, shall contain a high level summary of the Supplier's performance over the relevant Service Period, including details of the following:

(a) performance against its obligation to pay its Sub-contractors within thirty (30) days of receipt of an undisputed invoice;

(b) performance against its obligation to pay its Unconnected Sub-contractors within sixty (60) days of receipt of an invoice; and

(c) Social Value (as applicable).

1.6 The Performance Monitoring Report and the Balanced Scorecard Report shall be reviewed and their contents agreed by the Parties at the next Performance Review Meeting held in accordance with Paragraph 1.7.

1.7 The Parties shall attend meetings on a monthly basis (unless otherwise agreed) to review the Performance Monitoring Reports and the Balanced Scorecard Reports. The Performance Review Meetings shall (unless otherwise agreed):

(a) take place within 5 Working Days of the Performance Monitoring Report being issued by the Supplier;

(b) take place at such location and time (within normal business hours) as the Authority shall reasonably require (unless otherwise agreed in advance); and

(c) be attended by the Supplier Representative and the Authority Representative.

Final Performance Report

1.8 The Final Performance Monitoring Report shall be in such format as agreed between the Parties from time to time and contain, as a minimum, the following information as calculated at the end of the Term:

(a) for each Key Performance Indicator, the actual performance achieved by the Supplier;

(b) a summary of all KPI Failures;

(c) the severity level of each KPI Failure;

(d) the number of Service Points awarded in respect of each KPI Failure;

(e) the Service Credits to be applied (to the awarding body funding element only), indicating the KPI Failure(s) to which the Service Credits relate;

(f) the conduct and performance of any agreed periodic tests that have occurred, such as the annual failover test of the Service Continuity Plan;

(g) relevant particulars of any aspects of the Supplier's performance which fail to meet the requirements of this Agreement; and

(h) such other details as the Authority may reasonably require.

1.9 The Authority shall be entitled to raise any additional questions and/or request any further information from the Supplier regarding any KPI Failure.

Final Balanced Scorecard Report

1.10 The Balanced Scorecard Report shall be presented in the form of an accessible dashboard and, as a minimum, shall contain a high level summary of the Supplier's performance over the Term, including details of the following:

(a) performance against its obligation to pay its Sub-contractors within thirty (30) days of receipt of an undisputed invoice;

(b) performance against its obligation to pay its Unconnected Sub-contractors within sixty (60) days of receipt of an invoice; and

(c) Social Value (as applicable).

2 PERFORMANCE RECORDS

2.1 The Supplier shall keep appropriate documents and records (including, staff records, , training programmes, staff training records, goods received documentation, supplier accreditation records, complaints received etc) in relation to the Services being delivered. Without prejudice to the generality of the foregoing, the Supplier shall maintain accurate records of call histories for a minimum of 12 months and provide prompt access to such records to the Authority upon the Authority's request. The records and documents of the Supplier shall be available for inspection by the Authority and/or its nominee at any time and the Authority and/or its nominee may make copies of any such records and documents.

2.2 In addition to the requirement in Paragraph 2.1 to maintain appropriate documents and records, the Supplier shall provide to the Authority such supporting documentation as the Authority may reasonably require in order to verify the level of the performance of the Supplier both before and after the Service Commencement Date and the calculations of the amount of Service Credits.

2.3 The Supplier shall ensure that the Performance Monitoring Report, the Balanced Scorecard Report (as well as historic Performance Monitoring Reports and historic Balance Scorecard Reports) and any variations or amendments thereto, any reports and summaries produced in accordance

with this Schedule and any other document or record reasonably required by the Authority are available to the Authority on-line and are capable of being printed.

3 NOT USED

ANNEX 1: KEY PERFORMANCE INDICATORS

PART A: KEY PERFORMANCE INDICATORS

The Key Performance Indicators that shall apply to the Services are set out below:

1. Key Performance Indicators

No.	Key Performance Indicator Title	Definition	Frequency of Measurement	Severity Levels	Service Points	Publishable Performance Information
KPI1	Number of SLP CPD days delivered	Number of days of CPD delivered to teachers and support staff through the SLP programme	Progress against the KPI is reported monthly via the Performance Monitoring Report and Balanced	Target Performance Level: 100-90.0% of 24,782 days Minor KPI Failure: 89.9% - 85.0% Serious KPI Failure: 84.9% - 80.0%	0 1 2	YES – quarterly through Cabinet Office

			Scorecard Report. Performance against the KPI is measured at the end of the Term.	Severe KPI Failure: 79.9% - 75.0% KPI Service Threshold: below 75.0%	3 4	
KPI2	Number of SPN CPD days delivered	Number of days of CPD delivered to teachers or support staff through the SPN programme.	Progress against the KPI is reported monthly via the Performance Monitoring Report and Balanced Scorecard Report. Performance against the KPI is measured at the end of the Term.	Target Performance Level: 100-90.0% of 2,267 days Minor KPI Failure: 89.9% - 85.0% Serious KPI Failure: 84.9% - 80.0% Severe KPI Failure: 79.9% - 75.0% KPI Service Threshold: below 75.0%	0 1 2 3 4	YES – quarterly through Cabinet Office
KPI3	Schools that have completed	The (cumulative) number of schools that have completed their inclusion action plan	Progress towards KPI is reported	Target Performance Level: 100-85% of 100 schools	0	YES quarterly through Cabinet Office

	their Inclusion action plan		monthly via the Performance Monitoring Report and Balanced Scorecard Report. Performance against the KPI is measured at the end of the Term	Minor KPI Failure: 84.9% - 80.0% Serious KPI Failure: 79.9% - 75.0% Severe KPI Failure: 74.9% - 70.0% KPI Service Threshold: below 70.0%	1 2 3 4	
KPI4	Number of SKPT modules delivered	Total number of modules completed	Progress towards KPI is reported monthly via the Performance Monitoring Report and Balanced Scorecard Report. Performance against the KPI is	Target Performance Level: 100-85.0% of 800 modules Minor KPI Failure: 84.9% - 80.0% Serious KPI Failure: 79.9% - 75.0% Severe KPI Failure: 74.9% - 70.0%	0 1 2 3	YES quarterly through Cabinet Office

			measured at the end of the Term.	KPI Service Threshold: below 70.0%	4	
KPI5	Total number of CPD days provided for by bursaries	Number of days funded by bursaries	Progress towards KPI is reported monthly via the Performance Monitoring Report and Balanced Scorecard Report. Performance against the KPI is measured at the end of the Term.	Target Performance Level: 100-90.0% of 7,083 days Minor KPI Failure: 89.9% - 85.0% Serious KPI Failure: 84.9% - 80.0% Severe KPI Failure: 79.9% - 75.0% KPI Service Threshold: below 75.0%	Not applicable	NO
KPI6	Ensuring physical and mental health and wellbeing engagement is sufficient	% of employees who state that the physical and mental health and wellbeing engagement is sufficient directly due to the initiatives implemented under this Agreement	Progress towards KPI is reported monthly via the Performance Monitoring Report and Balanced	Target Performance Level: 100-70.0% of employees Minor KPI Failure: 69.9% - 60.0% Serious KPI Failure:	Not applicable	YES

			Scorecard Report. Performance against the KPI is measured at the end of the Term.	59.9% - 50.0% Severe KPI Failure: 49.9% - 35.0% KPI Service Threshold: below 75.0%		

PART B: NOT USED

MODEL AGREEMENT FOR SERVICES SCHEDULES

SCHEDULE 2.3

STANDARDS

Standards

1 DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

"Standards Hub"	the Government's open and transparent standards adoption process as documented at http://standards.data.gov.uk/; and
"Suggested Challenge"	a submission to suggest the adoption of new or emergent standards in the format specified on Standards Hub.

2 GENERAL

2.1 Throughout the term of this Agreement, the Parties shall monitor and notify each other of any new or emergent standards which could affect the Supplier's provision, or the Authority's receipt, of the Services. Any changes to the Standards, including the adoption of any such new or emergent standard, shall be agreed in accordance with the Change Control Procedure.

2.2 Where a new or emergent standard is to be developed or introduced by the Authority, the Supplier shall be responsible for ensuring that the potential impact on the Supplier's provision, or the Authority's receipt, of the Services is explained to the Authority (in a reasonable timeframe), prior to the implementation of the new or emergent standard.

2.3 Where Standards referenced conflict with each other or with Good Industry Practice, then the later Standard or best practice shall be adopted by the Supplier. Any such alteration to any Standard(s) shall require the prior written agreement of the Authority and shall be implemented within an agreed timescale.

3 TECHNOLOGY AND DIGITAL SERVICES PRACTICE

3.1 The Supplier shall (when designing, implementing and delivering the Services) adopt the applicable elements of HM Government's Technology Code of Practice as documented at https://www.gov.uk/service-manual/technology/code-of-practice.html.

4 OPEN DATA STANDARDS & STANDARDS HUB

4.1 The Supplier shall comply to the extent within its control with UK Government's Open Standards Principles as documented at https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles, as they relate to the specification of standards for software interoperability, data and document formats in the IT Environment.

4.2 Without prejudice to the generality of Paragraph 2.2, the Supplier shall, when implementing or updating a technical component or part of the Software or Supplier Solution where there is a requirement under this Agreement or opportunity to use a new or emergent standard, submit a Suggested

Challenge compliant with the UK Government's Open Standards Principles (using the process detailed on Standards Hub and documented at http://standards.data.gov.uk/). Each Suggested Challenge submitted by the Supplier shall detail, subject to the security and confidentiality provisions in this Agreement, an illustration of such requirement or opportunity within the IT Environment, Supplier Solution and Government's IT infrastructure and the suggested open standard.

4.3 The Supplier shall ensure that all documentation published on behalf of the Authority pursuant to this Agreement is provided in a non-proprietary format (such as PDF or Open Document Format (ISO 26300 or equivalent)) as well as any native file format documentation in accordance with the obligation under Paragraph 4.1 to comply with the UK Government's Open Standards Principles, unless the Authority otherwise agrees in writing.

5 TECHNOLOGY ARCHITECTURE STANDARDS

5.1 The Supplier shall produce full and detailed technical architecture documentation for the Supplier Solution in accordance with Good Industry Practice. If documentation exists that complies with the Open Group Architecture Framework 9.2 or its equivalent, then this shall be deemed acceptable.

6 ACCESSIBLE DIGITAL STANDARDS

6.1 The Supplier shall comply with (or with equivalents to):

(a) the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.1 Conformance Level AA; and

(b) ISO/IEC 13066-1: 2011 Information Technology – Interoperability with assistive technology (AT) – Part 1: Requirements and recommendations for interoperability.

7 SERVICE MANAGEMENT SOFTWARE & STANDARDS

7.1 Subject to Paragraphs 2 to 4 (inclusive), the Supplier shall reference relevant industry and HM Government standards and best practice guidelines in the management of the Services, including the following and/or their equivalents:

(a) ITIL v4;

(b) ISO/IEC 20000-1 2018 "Information technology — Service management – Part 1";

(c) ISO/IEC 20000-2 2019 "Information technology — Service management – Part 2";

(d) ISO/IEC 27001/27002 "Information security management"

(e) ISO 10007: 2017 "Quality management systems – Guidelines for configuration management"; and

(f) ISO 22313:2020 “Security and resilience. Business continuity management systems. Guidance on the use of ISO 22301” and, ISO/IEC 27031:2011 and ISO 22301:2019.

7.2 For the purposes of management of the Services and delivery performance the Supplier shall make use of Software that complies with Good Industry Practice including availability, change, incident, knowledge, problem, release & deployment, request fulfilment, service asset and configuration, service catalogue, service level and service portfolio management. If such Software has been assessed under the ITIL Software Scheme as being compliant to “Bronze Level”, then this shall be deemed acceptable.

8 NOT USED

9 HARDWARE SAFETY STANDARDS

9.1 The Supplier shall comply with those BS or other standards relevant to the provision of the Services, including the following or their equivalents:

(a) any new hardware required for the delivery of the Services (including printers), shall conform to BS EN IEC 62368-1:2020+A11:2020 or subsequent replacements. In considering where to site any such hardware, the Supplier shall consider the future working user environment and shall position the hardware sympathetically, wherever possible;

(b) any new audio, video and similar electronic apparatus required for the delivery of the Services, shall conform to the following standard: BS EN IEC 62368-1:2020+A11:2020 or any subsequent replacements;

(c) any new laser printers or scanners using lasers, required for the delivery of the Services, shall conform to either of the following safety Standards: BS EN 60825-1:2014 or any subsequent replacements; and

(d) any new apparatus for connection to any telecommunication network, and required for the delivery of the Services, shall conform to the following safety Standard: BS EN 62949:2017 or any subsequent replacements.

9.2 Where required to do so as part of the Services, the Supplier shall perform electrical safety checks in relation to all equipment supplied under this Agreement in accordance with the relevant health and safety regulations.

MODEL AGREEMENT FOR SERVICES SCHEDULES

SCHEDULE 2.4

SECURITY MANAGEMENT

PART A: SECURITY ASSURANCE

1 Definitions

1.1 In this Schedule:

"Anti-Malicious Software"	means software that scans for and identifies possible Malicious Software in the IT Environment;
"Breach of Security	an event that results, or could result, in: (a) any unauthorised access to or use of the Authority Data, the Services and/or the Information Management System; and/or (b) the loss, corruption and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including any copies of such information or data, used by the Authority and/or the Supplier in connection with this Agreement;
"Certification Requirements"	means the information security requirements set out in Paragraph 6;
"CHECK Service Provider"	means a company which has been certified by the National Cyber Security Centre, holds "Green Light" status and is authorised to provide the IT Health Check services required by Paragraph 7.1;
"CREST Service Provider"	means a company with a SOC Accreditation from CREST International;
"Higher Risk Sub-contractor"	means a Sub-contractor that Processes Authority Data , where that data includes either: (a) the Personal Data of 1000 or more individuals in aggregate during the period between the Service Commencement Date and the date on which this Agreement terminates in accordance with Clause 4.1(b); or (b) Special Category Personal Data;
"Cyber Essentials"	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;

"Cyber Essentials Plus"	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Scheme"	means the Cyber Essentials scheme operated by the National Cyber Security Centre;
"Incident Management Process"	means the process which the Supplier shall implement immediately after it becomes aware of a Breach of Security which is intended to restore normal operations as quickly as possible, minimising any adverse impact on the Authority Data, the Authority, the Services and/or users of the Services and which shall be shall be prepared by the Supplier in accordance with Paragraph 4 using the template set out in Annex 3.;
"Information Assurance Assessment"	means the set of policies, procedures, systems and processes which the Supplier shall implement, maintain and update in accordance with Paragraph 4 in order to manage, mitigate and, where possible, avoid information security risks including cyber-attacks, hacks, data leaks, Personal Data Breaches and/or theft and which shall be prepared by the Supplier using the template set out in Annex 3.;
"Information Management System"	means (a) those parts of the Supplier System, and those of the Sites, that the Supplier or its Sub-contractors will use to provide the parts of the Services that require Processing Authority Data; and (b) the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources);
"Information Security Approval Statement"	means a notice issued by the Authority which sets out the information risks which the Supplier has identified as being associated with using the Information Management System and confirms that: (a) the Authority is satisfied that the identified risks have been adequately and appropriately addressed;

(b) the Authority has accepted the residual risks; and

(c) the Supplier may use the Information Management System to Process Authority Data;

"IT Health Check" has the meaning given in Paragraph 7.1;

"Medium Risk Sub-contractor" means a Sub-contractor that Processes Authority Data, where that data

(a) includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the Service Commencement Date and the date on which this Agreement terminates in accordance with Clause 4.1(b); and

(b) does not include Special Category Personal Data;

"Personal Data Processing Statement" means a document setting out:

(a) the types of Personal Data which the Supplier and/or its Sub-contractors Processes or will Process under this Agreement;

(b) the categories of Data Subjects whose Personal Data the Supplier and/or its Sub-contractors Processes or will Process under this Agreement;

(c) the nature and purpose of such Processing;

(d) the locations at which the Supplier and/or its Sub-contractors Process Personal Data under this Agreement; and

(e) the Protective Measures that the Supplier and, where applicable, its Sub-contractors have implemented to protect Personal Data Processed under this Agreement against a Breach of Security (insofar as that Breach of Security relates to data) or a Personal Data Breach;

"Process" means any operation which is performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

	dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"Required Changes Register"	mean the register within the Security Management Plan which is to be maintained and updated by the Supplier and which shall record each of the changes that the Supplier shall make to the Information Management System and/or the Security Management Plan as a consequence of the occurrence of any of the events set out in Paragraph 5.2 together with the date by which such change shall be implemented and the date on which such change was implemented;
"Risk Register"	is the risk register within the Information Assurance Assessment which is to be prepared and submitted to the Authority for approval in accordance with Paragraph 4;
"Security Management Plan"	means the document prepared by the Supplier using the template in Annex 3, comprising: (a) the Information Assurance Assessment; (b) the Personal Data Processing Statement; (c) the Required Changes Register; and (d) the Incident Management Process;
Special Category Personal Data	means the categories of Personal Data set out in article 9(1) of the GDPR;

2 Introduction

2.1 This Schedule sets out:

(a) the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Agreement to ensure the security of the Authority Data and the Information Management System;

(b) the Certification Requirements applicable to the Supplier and each of those Sub-contractors which Processes Authority Data;

(c) The security requirements in Annex 1, with which the Supplier must comply;

(d) the tests which the Supplier shall conduct on the Information Management System during the Term;

(e) the Supplier's obligations to:

(i) return or destroy Authority Data on the expiry or earlier termination of this Agreement; and

(ii) prevent the introduction of Malicious Software into the Supplier System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Supplier System in Paragraph 9; and

(iii) report Breaches of Security to the Authority.

3 Principles of Security

3.1 The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Authority Data and, consequently on the security of:

(a) the Sites;

(b) the IT Environment;

(c) the Information Management System; and

(d) the Services.

3.2 Notwithstanding the involvement of the Authority in assessing the arrangements which the Supplier implements to ensure the security of the Authority Data and the Information Management System, the Supplier shall be, and shall remain, responsible for:

(a) the security, confidentiality, integrity and availability of the Authority Data whilst that Authority Data is under the control of the Supplier or any of its Sub-contractors; and

(b) the security of the Information Management System.

3.3 The Supplier shall:

(a) comply with the security requirements in Annex 1; and

(b) ensure that each Sub-contractor that Processes Authority Data complies with the Sub-contractor Security Requirements.

3.4 The Supplier shall provide the Authority with access to Supplier Personnel responsible for information assurance to facilitate the Authority's assessment of the Supplier's compliance with its obligations set out in this Schedule at reasonable times on reasonable notice.

4 Information Security Approval Statement

4.1 The Supplier must ensure that it has provided the Authority with such documentation as the Authority has notified that it requires which sets out how it will ensure compliance with the requirements of this Schedule, including any

requirements imposed on Sub-contractors by Annex 2, from the Services Commencement Date.

4.2 The Supplier may not use the Information Management System to Process Authority Data unless and until:

(a) the Supplier has procured the conduct of an IT Health Check of the Supplier System by a CHECK Service Provider or a CREST Service Provider in accordance with Paragraph 7.1; and

(b) the Authority has issued the Supplier with an Information Security Approval Statement in accordance with the process set out in this Paragraph 4.

4.3 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Schedule and the Agreement in order to ensure the security of the Authority Data and the Information Management System.

4.4 The Supplier shall prepare and submit to the Authority within 20 Working Days of the date of this Agreement, the Security Management Plan, which comprises:

(a) an Information Assurance Assessment;

(b) the Required Changes Register;

(c) the Personal Data Processing Statement; and

(d) the Incident Management Process.

4.5 The Authority shall review the Supplier's proposed Security Management Plan as soon as possible and, in any event within 20 Working Days of receipt and shall either issue the Supplier with:

(a) an Information Security Approval Statement, which shall confirm that the Supplier may use the Information Management System to Process Authority Data; or

(b) a rejection notice, which shall set out the Authority's reasons for rejecting the Security Management Plan.

4.6 If the Authority rejects the Supplier's proposed Security Management Plan, the Supplier shall take the Authority's reasons into account in the preparation of a revised Security Management Plan, which the Supplier shall submit to the Authority for review within 10 Working Days or such other timescale as agreed with the Authority.

4.7 The Authority may require, and the Supplier shall provide the Authority and its authorised representatives with:

(a) access to the Supplier Personnel;

(b) access to the Information Management System to audit the Supplier and its Sub-contractors' compliance with this Agreement; and

(c) such other information and/or documentation that the Authority or its authorised representatives may reasonably require,

to assist the Authority to establish whether the arrangements which the Supplier and its Sub-contractors have implemented in order to ensure the security of the Authority Data and the Information Management System are consistent with the representations in the Security Management Plan. The Supplier shall provide the access required by the Authority in accordance with this Paragraph within 10 Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Authority with the access that it requires within 24 hours of receipt of such request.

5 Compliance Reviews

5.1 The Supplier shall regularly review and update the Security Management Plan, and provide such to the Authority, at least once each year and as required by this Paragraph.

5.2 The Supplier shall notify the Authority within 2 Working Days after becoming aware of:

(a) a significant change to the components or architecture of the Information Management System;

(b) a new risk to the components or architecture of the Information Management System;

(c) a vulnerability to the components or architecture of the Service which is classified 'Medium', 'High', 'Critical' or 'Important' in accordance with the classification methodology set out in Paragraph .2 of Annex 1 to this Schedule;

(d) a change in the threat profile;

(e) a significant change to any risk component;

(f) a significant change in the quantity of Personal Data held within the Service;

(g) a proposal to change any of the Sites from which any part of the Services are provided; and/or

(h) an ISO27001 audit report and/or Cyber Essentials PLUS produced in connection with the Certification Requirements indicates significant concerns.

5.3 Within 10 Working Days of such notifying the Authority or such other timescale as may be agreed with the Authority, the Supplier shall make the necessary changes to the Required Changes Register and submit the updated Required Changes Register the Authority for review and approval.

5.4 Where the Supplier is required to implement a change, including any change to the Information Management System, the Supplier shall effect such change at its own cost and expense.

6 Certification Requirements

6.1 The Supplier shall be certified as compliant with:

(a) ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

(b) Cyber Essentials PLUS,

and shall provide the Authority with a copy of each such certificate of compliance before the Supplier shall be permitted to receive, store or Process Authority Data.

6.2 The Supplier shall ensure that each Higher Risk Sub-contractor is certified as compliant with either:

(a) ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; or

(b) Cyber Essentials PLUS,

and shall provide the Authority with a copy of each such certificate of compliance before the Higher-Risk Sub-contractor shall be permitted to receive, store or Process Authority Data.

6.3 The Supplier shall ensure that each Medium Risk Sub-contractor is certified compliant with Cyber Essentials.

6.4 The Supplier shall ensure that the Supplier and each Sub-contractor who is responsible for the secure destruction of Authority Data:

(a) securely destroys Authority Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and

(b) are certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the Authority.

6.5 The Supplier shall provide the Authority with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph 6 before the Supplier or the relevant Sub-contractor (as applicable) may carry out the secure destruction of any Authority Data.

6.6 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier or any Sub-contractor

ceases to be compliant with the Certification Requirements and, on request from the Authority, shall or shall procure that the relevant Sub-contractor shall:

(a) immediately ceases using the Authority Data; and

(b) procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Authority Data in accordance with the requirements set out in this Paragraph.

(c) The Authority may agree to exempt, in whole or part, the Supplier or any Sub-contractor from the requirements of this Paragraph 6. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Management Plan.

7 Security Testing

7.1 The Supplier shall, at its own cost and expense procure and conduct:

(a) testing of the Information Management System by a CHECK Service Provider or a CREST Service Provider ("**IT Health Check**"); and

(b) such other security tests as may be required by the Authority,

7.2 The Supplier shall complete all of the above security tests before the Supplier submits the Security Management Plan to the Authority for review in accordance with Paragraph 4; and it shall repeat the IT Health Check not less than once every 12 months during the Term and submit the results of each such test to the Authority for review in accordance with this Paragraph.

7.3 In relation to each IT Health Check, the Supplier shall:

(a) agree with the Authority the aim and scope of the IT Health Check;

(b) promptly, and no later than ten (10) Working Days, following the receipt of each IT Health Check report, provide the Authority with a copy of the full report;

(c) in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:

(i) prepare a remedial plan for approval by the Authority (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the IT Health Check report:

(A) how the vulnerability will be remedied;

(B) unless otherwise agreed in writing between the Parties, the date by which the vulnerability will be remedied, which must be:

(1) within three months of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of "medium";

(2) within one month of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “high”; and

(3) within 10 Working Days of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “critical”;

(C) the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Authority, include a further IT Health Check) to confirm that the vulnerability has been remedied;

(ii) comply with the Vulnerability Correction Plan; and

(iii) conduct such further tests on the Service as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.

7.4 The Supplier shall ensure that any testing which could adversely affect the Supplier System shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such tests shall be agreed in advance with the Authority.

7.5 If any testing conducted by or on behalf of the Supplier identifies a new risk, new threat, vulnerability or exploitation technique that has the potential to affect the security of the Information Management System, the Supplier shall within 2 Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique provide the Authority with a copy of the test report and:

(a) propose interim mitigation measures to vulnerabilities in the Information Management System known to be exploitable where a security patch is not immediately available; and

(b) where and to the extent applicable, remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Supplier System) within the timescales set out in the test report or such other timescales as may be agreed with the Authority.

7.6 The Supplier shall conduct such further tests of the Supplier System as may be required by the Authority from time to time to demonstrate compliance with its obligations set out this Schedule and the Agreement.

7.7 The Supplier shall notify the Authority immediately if it fails to, or believes that it will not, mitigate the vulnerability within the timescales set out in Annex 1 to this Schedule.

8 Security Monitoring and Reporting

8.1 The Supplier shall:

(a) monitor the delivery of assurance activities;

(b) maintain and update the Security Management Plan in accordance with Paragraph 5;

(c) agree a document which presents the residual security risks to inform the Authority's decision to give approval to the Supplier to Process, store and transit the Authority Data;

(d) monitor security risk impacting upon the operation of the Service;

(e) report Breaches of Security in accordance with the approved Incident Management Process;

(f) agree with the Authority the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Authority within 20 Working Days of date of this Agreement.

9 Malicious Software

9.1 The Supplier shall install and maintain Anti-Malicious Software or procure that Anti-Malicious Software is installed and maintained on any part of the Information Management System which may Process Authority Data and ensure that such Anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the Information Management System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Information Management System, to identify, contain the spread of, and minimise the impact of Malicious Software.

9.2 If Malicious Software is found, the parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

9.3 Any cost arising out of the actions of the parties taken in compliance with the provisions of Paragraph 9.2 shall be borne by the parties as follows:

(a) by the Supplier where the Malicious Software originates from the Supplier Software, the Third Party Software supplied by the Supplier or the Authority Data (whilst the Authority Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Authority when provided to the Supplier; and

(b) by the Authority, in any other circumstance.

10 Breach of Security

10.1 If either party becomes aware of a Breach of Security it shall notify the other in accordance with the Incident Management Process.

10.2 The Incident Management Process shall, as a minimum, require the Supplier to do the following upon it becoming aware of a Breach of Security or attempted Breach of Security:

(a) Immediately take all reasonable steps necessary to:

(i) minimise the extent of actual or potential harm caused by such Breach of Security;

(ii) remedy such Breach of Security to the extent possible;

(iii) apply a tested mitigation against any such Breach of Security; and

(iv) prevent a further Breach of Security in the future which exploits the same root cause failure;

(b) as soon as reasonably practicable and, in any event, within 2 Working Days, following the Breach of Security or attempted Breach of Security, provide to the Authority full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.

10.3 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance by the Supplier, its Sub-contractors and/or all or any part of the Information Management System with this Agreement, then such remedial action shall be completed at no additional cost to the Authority.

ANNEX 1: SECURITY REQUIREMENTS

1 Security Classification of Information

1.1 If the provision of the Services requires the Supplier to Process Authority Data which is classified as OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

2 End User Devices

2.1 The Supplier shall ensure that any Authority Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Authority except where the Authority has given its prior written consent to an alternative arrangement.

2.2 The Supplier shall ensure that any device which is used to Process Authority Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/collection/end-user-device-security.

3 Networking

3.1 The Supplier shall ensure that any Authority Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

4 Personnel Security

4.1 All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record.

4.2 The Authority and the Supplier shall review the roles and responsibilities of the Supplier Personnel who will be involved in the management and/or provision of the Services in order to enable the Authority to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Authority Data or data which, if it were Authority Data, would be classified as OFFICIAL-SENSITIVE.

4.3 The Supplier shall not permit Supplier Personnel who fail the security checks required by Paragraphs .1 and .2 to be involved in the management and/or

provision of the Services except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.

4.4 The Supplier shall ensure that Supplier Personnel are only granted such access to Authority Data as is necessary to enable the Supplier Personnel to perform their role and to fulfil their responsibilities.

4.5 The Supplier shall ensure that Supplier Personnel who no longer require access to the Authority Data (e.g. they cease to be employed by the Supplier or any of its Sub-contractors), have their rights to access the Authority Data revoked within 1 Working Day.

4.6 The Supplier shall ensure that Supplier Staff that have access to the Sites, the IT Environment or the Authority Data receive regular training on security awareness that reflects the degree of access those individuals have to the Sites, the IT Environment or the Authority Data.

4.7 The Supplier shall ensure that the training provided to Supplier Staff under paragraph .6 includes training on the identification and reporting fraudulent communications intended to induce individuals to disclose Personal Data or any other information that could be used, including in combination with other Personal Data or information, or with other techniques, to facilitate unauthorised access to the Sites, the IT Environment or the Authority Data ("phishing").

5 Identity, Authentication and Access Control

5.1 The Supplier shall operate an access control regime to ensure:

(a) all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and

(b) all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.

5.2 The Supplier shall apply the 'principle of least privilege' when allowing persons access to the Supplier System and Sites so that such persons are allowed access only to those parts of the Sites and the Supplier System they require.

5.3 The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such record available to the Authority on request.

6 Data Destruction or Deletion

6.1 The Supplier shall:

(a) The Supplier shall: prior to securely sanitising any Authority Data or when requested the Supplier shall provide the Government with all Authority Data in an agreed open format;

(b) have documented processes to ensure the availability of Authority Data in the event of the Supplier ceasing to trade;

(c) securely erase in a manner agreed with the Authority any or all Authority Data held by the Supplier when requested to do so by the Authority;

(d) securely destroy in a manner agreed with the Authority all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in this Agreement and, in the absence of any such requirements, as agreed by the Authority; and

(e) implement processes which address the CPNI and NCSC guidance on secure sanitisation.

7 Audit and Protective Monitoring

7.1 The Supplier shall collect audit records which relate to security events in the Information Management System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the Information Management System, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data.

7.2 The Supplier and the Authority shall work together to establish any additional audit and monitoring requirements for the Information Management System.

7.3 The retention periods for audit records and event logs must be agreed with the Authority and documented in the Security Management Plan.

8 Location of Authority Data

8.1 The Supplier shall not and shall procure that none of its Sub-contractors Process Authority Data outside the United Kingdom without the prior written consent of the Authority, which may be subject to conditions.

9 Vulnerabilities and Corrective Action

9.1 The Authority and the Supplier acknowledge that from time to time vulnerabilities in the Information Management System will be discovered which unless mitigated will present an unacceptable risk to the Authority Data.

9.2 The severity of vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the Security Management Plan and using the appropriate vulnerability scoring systems including:

(a) the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST at http://nvd.nist.gov/cvss.cfm); and

(b) Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

9.3 Subject to Paragraph .4, the Supplier shall procure the application of security patches to vulnerabilities in the Information Management System within:

(a) seven (7) days after the public release of patches for those vulnerabilities categorised as 'Critical';

(b) thirty (30) days after the public release of patches for those vulnerabilities categorised as 'Important'; and

(c) sixty (60) days after the public release of patches for those vulnerabilities categorised as 'Other'.

9.4 The timescales for applying patches to vulnerabilities in the Information Management System set out in Paragraph .3 shall be extended where:

(a) the Supplier can demonstrate that a vulnerability in the Information Management System is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the timescales set out in Paragraph .3 if the vulnerability becomes exploitable within the context of the Services;

(b) the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of five (5) days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or

(c) the Authority agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Security Management Plan.

9.5 The Security Management Plan shall include provisions for major version upgrades of all COTS Software to be kept up to date such that all COTS Software are always in mainstream support throughout the Term unless otherwise agreed by the Authority in writing. All COTS Software should be no more than N-1 versions behind the latest software release.

10 Secure Architecture

10.1 The Supplier shall design the Information Management System in accordance with:

(a) the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main;

(b) the NCSC "Bulk Data Principles", a copy of which can be found at https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main; and

(c) the NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles and which are summarised below:

(i) "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;

(ii) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;

(iii) "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;

(iv) "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Services and information within it;

(v) "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;

(vi) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Personnel have access to Authority Data and/or the Authority System that those personnel be subject to appropriate security screening and regular security training;

(vii) "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;

(viii) "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Sub-contractors and other suppliers;

(ix) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the

tools available for the Authority to securely manage the Authority's use of the Service;

(x) "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;

(xi) "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;

(xii) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;

(xiii) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Authority with the audit records it needs to monitor access to the Service and the Authority Data held by the Supplier and/or its Sub-contractors; and

(xiv) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Personnel on the safe and secure use of the Information Management System.

ANNEX 2: SECURITY REQUIREMENTS FOR SUB-CONTRACTORS

1 Application of Annex

1.1 This Annex applies to all Sub-contractors that Process Authority Data.

1.2 The Supplier must:

(a) ensure that those Sub-contractors comply with the provisions of this Annex; and

(b) keep sufficient records to demonstrate that compliance to the Authority; and

2 Designing and managing secure solutions

2.1 The Sub-contractor shall implement their solution(s) to mitigate the security risks in accordance with the NCSC's Cyber Security Design Principles https://www.ncsc.gov.uk/collection/cyber-security-design-principles.

2.2 The Sub-contractor must assess their systems against the NCSC Cloud Security Principles: https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-contractor must document that assessment and make that documentation available to the Authority on the Authority's request.

3 Data Processing, Storage, Management and Destruction

3.1 The Sub-contractor must not Process any Authority Data outside the United Kingdom. The Authority may permit the Sub-contractor to Process Authority Data outside the United Kingdom and may impose conditions on that permission, with which the Sub-contractor must comply. Any permission must be in writing to be effective.

3.2 The Sub-contractor must securely erase any or all Authority Data held by the Sub-contractor when requested to do so by the Authority; and securely destroy all media that has held Authority Data at the end of life of that media in accordance with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard, or an alternative agreed in writing by the Authority.

4 Personnel Security

4.1 The Sub-contractor must perform appropriate checks on their staff before they may participate in the provision and or management of the Services. Those checks must include all pre-employment checks required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record. The HMG Baseline Personnel Security Standard is at https://www.gov.uk/government/publications/government-baseline-personnel-security-standard.

4.2 The Sub-contractor must, if the Authority requires, at any time, ensure that one or more of the Sub-contractor's staff obtains Security Check clearance in order to Process Authority Data containing Personal Data above certain volumes specified by the Authority, or containing Special Category Personal Data.

4.3 Any Sub-contractor staff who will, when performing the Services, have access to a person under the age of 18 years must undergo Disclosure and Barring Service checks.

5 End User Devices

5.1 The Sub-contractor shall ensure that any Authority Data stored (for any period of time) on a mobile, removable or physically uncontrolled device is encrypted. The Sub-contractor must follow the Information Commissioner's Office guidance on implementing encryption, which can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/.

5.2 The Supplier shall ensure that any device used to Process Authority Data meets all the security requirements set out in the NCSC End User Devices Platform Security Guidance, which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security.

6 Networking

6.1 The Supplier shall ensure that any Authority Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

7 Patching and Vulnerability Scanning

7.1 The Sub-contractor must proactively monitor supplier vulnerability websites and ensure all necessary patches and upgrades are applied to maintain security, integrity and availability in accordance with the NCSC Cloud Security Principles.

8 Third Party Sub-contractors

8.1 The Sub-contractor must not transmit or disseminate the Authority Data to any other person unless specifically authorised by the Authority. Such authorisation must be in writing to be effective and may be subject to conditions.

8.2 The Sub-contractor must not, when performing any part of the Services, use any software to Process the Authority Data where the licence terms of that software purport to grant the licensor rights to Progress the Authority Data greater than those rights strictly necessary for the use of the software.

ANNEX 3: SECURITY MANAGEMENT PLAN TEMPLATE

Security Management Plan Template (Accreditation)

Science CPD Programme – England STEM Learning Limited

1 Executive Summary

<This section should contain a brief summary of the business context of the system, any key IA controls, the assurance work done, any off-shoring considerations and any significant residual risks that need acceptance.>

2 System Description

2.1 Background

< A short description of the project/product/system. Describe its purpose, functionality, aim and scope.>

2.2 Organisational Ownership/Structure

<Who owns the system and operates the system and the organisational governance structure. This should include how any ongoing security management is integrated into the project governance e.g. how a Security Working Group reports to the project board.>

2.3 Information assets and flows

<The information assets processed by the system which should include a simple high level diagram on one page. Include a list of the type and volumes of data that will be processed, managed and stored within the supplier system. If personal data, please include the fields used such as name, address, department DOB, NI number etc.>

2.4 System Architecture

<A description of the physical system architecture, to include the system management. A diagram will be needed here>

2.5 Users

<A brief description of the system users, to include HMG users as well as any service provider users and system managers. If relevant, security clearance level requirements should be included.>

2.6 Locations

<Where the data assets are stored and managed from. If any locations hold independent security certifications (e.g. ISO27001:2013) these should be noted. Any off-shoring considerations should be detailed.>

2.7 Test and Development Systems

<Include information about any test and development systems, their locations and whether they contain live system data.>

2.8 Key roles and responsibilities

<A brief description of the lead security roles such as that of the SIRO, IAO, Security manager, Accreditor >

3 Risk Assessment

3.1 Accreditation/Assurance Scope

<This section describes the scope of the Accreditation/Assurance for the system. The scope of the assurance assessment should be clearly indicated, with components of the architecture upon which reliance is placed but assurance will not be done clearly shown e.g. a cloud hosting service. A logical diagram should be used along with a brief description of the components.>

3.2 Risk appetite

<A risk appetite should be agreed with the SIRO/SRO and included here.>

3.3 Business impact assessment

< A description of the information assets and the impact of their loss or corruption (e.g. large amounts of Official Sensitive personal data the loss of which would be severely damaging to individuals, embarrassing to HMG, and make HMG liable to ICO investigations) in business terms should be included. This section should cover the impact on loss of confidentiality, integrity and availability of the assets. The format of this assessment may be dependent on the risk assessment method chosen.>

3.4 Risk assessment

<The content of this section will depend on the risk assessment methodology chosen, but should contain the output of the formal information risk assessment in a prioritised list using business language. Experts on the system and business process should have been involved in the risk assessment to ensure the formal risk methodology used has not missed out any risks. The example table below should be used as the format to identify the risks and document the controls used to mitigate those risks. >

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R1	Internet attackers could hack the system.	Medium	The service systems are exposed to the internet via the web portal.	C1: Internet-facing firewalls	Very low

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
				C2: Internet-facing IP whitelist C3: System hardening C4: Protective monitoring C5: Application access control C16: Anti-virus for incoming files C54: Files deleted when processed C59: Removal of departmental identifier	
R2	Remote attackers could intercept or disrupt information crossing the internet.	Medium	File sharing with organisations across the internet.	C9: TLS communications C10: PGP file-sharing	Very low
R3	Internal users could maliciously or accidentally alter bank details.	Medium-High	Users bank details can be altered as part of the normal business function.	C12. System administrators hold SC clearance. C13. All changes to user information are logged and audited. C14. Letters are automatically sent to users home	Low

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
				addresses when bank details are altered. C15. Staff awareness training	

3.5 Controls

<The controls listed above to mitigate the risks identified should be detailed. There should be a description of each control, further information and configuration details where relevant, and an assessment of the implementation status of, and assurance in, the control. A sample layout is included below.>

ID	Control title	Control description	Further information and assurance status
C1	Internet-facing firewalls	Internet-facing firewalls are in place between the internet and the system', which restrict access from the internet to the required ports only.	Assured via ITHC firewall rule check
C2	Internet-facing IP whitelist	An IP whitelist is in place for all access from the internet.	Assured via ITHC
C15	Staff awareness training	All staff must undertake annual security awareness training and this process is audited and monitored by line managers.	Assured as part of ISO27001 certification

3.6 Residual risks and actions

<A summary of the residual risks which are likely to be above the risk appetite stated after all controls have been applied and verified should be listed with actions and timescales included.>

4 In-service controls

< This section should describe the controls relating to the information lifecycle, including development, testing, in-service, termination and on-going risk management and accreditation assurance. Details of any formal assurance requirements specified in the contract such as security CHECK testing or maintained ISO27001 certification should be included. This section should include at least:

(c) information risk management and timescales and triggers for a review;

(d) contractual patching requirements and timescales for the different priorities of patch;

(e) protective monitoring arrangements to include how anomalous behaviour is identified and acted upon as well as how logging and auditing of user activity is done;

(f) configuration and change management;

(g) incident management;

(h) vulnerability management;

(i) user access management; and

(j) data sanitisation and disposal.>

5 Security Operating Procedures (SyOPs)

< If needed any SyOps requirements should be included and referenced here.>

6 Major Hardware and Software and end of support dates

< This should be a table which lists the end of support dates for hardware and software products and components. An example table is shown below.>

Name	Version	End of mainstream Support/Extended Support	Notes/RAG Status
Server Host	HP XXXX	Feb 2020/ March 2022	

7 Incident Management Process

<The suppliers' process, as agreed with the Authority/Customer, should be included here. It must as a minimum include the protocol for how and when incidents will be reported to the Authority/customer and the process that will be undertaken to mitigate the incidents and investigate the root cause.>

8 Security Requirements for User Organisations

<Any security requirements for connecting organisations or departments should be included or referenced here.>

9 Required Changes Register

<The table below shows the headings for the Required Changes Register which should be maintained and used to update the contents of this document at least annually.>

Ref	Section	Change	Agreed With	Date agreed	Documentation update	Status
1	6.4	A new Third Party supplier XXXX will be performing the print capability.	Authority name	11/11/2018	Jul-2019	Open

10 Personal Data Processing Statement

<This should include: (i) the types of Personal Data which the Supplier and/or its Sub-contractors are Processing on behalf of the Authority; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Sub-contractors are Processing on behalf of the Authority; the nature and purpose of such Processing; (iii) the locations at which the Supplier and/or its Subcontractors Process Authority Data; and, (iv) the Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect the Authority Data against a Security Breach including a Personal Data Breach.>

11 Annex A. ISO27001 and/or Cyber Essential Plus certificates

<Any certifications relied upon should have their certificates included>

12 Annex B. Cloud Security Principles assessment

<A spreadsheet may be attached>

13 Annex C. Protecting Bulk Data assessment if required by the Authority/Customer

<A spreadsheet may be attached>

14 Annex E. Latest ITHC report and Vulnerability Correction Plan

MODEL AGREEMENT FOR SERVICES SCHEDULES

SCHEDULE 2.5

INSURANCE REQUIREMENTS

1 OBLIGATION TO MAINTAIN INSURANCES

1.1 Without prejudice to its obligations to the Authority under this Agreement, including its indemnity and liability obligations, the Supplier shall for the periods specified in this Schedule take out and maintain, or procure the taking out and maintenance of the insurances as set out in Annex 1 and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than the date on which the relevant risk commences.

1.2 The Insurances shall be maintained in accordance with Good Industry Practice and (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time.

1.3 The Insurances shall be taken out and maintained with insurers who are:

(a) of good financial standing;

(b) appropriately regulated;

(c) regulated by the applicable regulatory body and is in good standing with that regulator; and

(d) except in the case of any Insurances provided by an Affiliate of the Supplier, of good repute in the international insurance market.

1.4 The Supplier shall ensure that the public and products liability policy shall contain an indemnity to principals clause under which the Authority shall be indemnified in respect of claims made against the Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Agreement and for which the Supplier is legally liable.

2 GENERAL OBLIGATIONS

2.1 Without limiting the other provisions of this Agreement, the Supplier shall:

(a) take or procure the taking of all reasonable risk management and risk control measures in relation to the Services as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;

(b) promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

(c) hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

3 FAILURE TO INSURE

3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.

3.2 Where the Supplier has failed to purchase any of the Insurances or maintain any of the Insurances in full force and effect, the Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances, and the Authority shall be entitled to recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4 EVIDENCE OF INSURANCES

4.1 The Supplier shall upon the Effective Date and within 15 Working Days after the renewal or replacement of each of the Insurances, provide evidence, in a form satisfactory to the Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule. Receipt of such evidence by the Authority shall not in itself constitute acceptance by the Authority or relieve the Supplier of any of its liabilities and obligations under this Agreement.

5 CANCELLATION

5.1 Subject to Paragraph 5.2, the Supplier shall notify the Authority in writing at least 5 Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.

5.2 Without prejudice to the Supplier's obligations under Paragraph 4, Paragraph 5.1 shall not apply where the termination of any Insurances occurs purely as a result of a change of insurer in respect of any of the Insurances required to be taken out and maintained in accordance with this Schedule.

6 INSURANCE CLAIMS, PREMIUMS AND DEDUCTIBLES

6.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Services and/or this Agreement for which it may be entitled to claim under any of the Insurances. In the event that the Authority receives a claim relating to or arising out of the Services and/or this Agreement, the Supplier shall co-operate with the Authority and assist it in dealing with such claims at its own expense including without limitation providing information and documentation in a timely manner.

6.2 The Supplier shall maintain a register of all claims under the Insurances in connection with this Agreement and shall allow the Authority to review such register at any time.

6.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

6.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Agreement or otherwise.

ANNEX 1: REQUIRED INSURANCES

PART A: INSURANCE CLAIM NOTIFICATION

Except where the Authority is the claimant party, the Supplier shall give the Authority notice within 20 Working Days after any insurance claim in excess of [redacted] relating to or arising out of the provision of the Services or this Agreement on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Authority) full details of the incident giving rise to the claim.

PART B: THIRD PARTY PUBLIC LIABILITY INSURANCE

1 Insured

1.1 The Supplier (the "Insured")

2 Interest

2.1 To indemnify the Insured in respect of all sums which the Insured shall become legally liable to pay as damages, including claimant's costs and expenses, in respect of accidental:

(a) death or bodily injury to or sickness, illness or disease contracted by any person; and

(b) loss of or damage to physical property;

happening during the period of insurance (as specified in Paragraph 5) and arising out of or in connection with the provision of the Services and in connection with this Agreement.

3 Limit of indemnity

3.1 Not less than [redacted] in respect of any one occurrence, the number of occurrences being unlimited in any annual policy period.

4 Territorial limits

4.1 United Kingdom

5 Period of insurance

5.1 From the date of this Agreement for the Term and renewable on an annual basis unless agreed otherwise by the Authority in writing.

6 Cover features and extensions

6.1 Indemnity to principals clause under which the Authority shall be indemnified in respect of claims made against the Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Agreement and for which the Supplier is legally liable.

7 Principal exclusions

7.1 War and related perils.

7.2 Nuclear and radioactive risks.

7.3 Liability for death, illness, disease or bodily injury sustained by employees of the Insured arising out of the course of their employment.

7.4 Liability arising out of the use of mechanically propelled vehicles whilst required to be compulsorily insured by applicable Law in respect of such vehicles.

7.5 Liability in respect of predetermined penalties or liquidated damages imposed under any contract entered into by the Insured.

7.6 Liability arising out of technical or professional advice other than in respect of death or bodily injury to persons or damage to third party property.

7.7 Liability arising from the ownership, possession or use of any aircraft or marine vessel.

7.8 Liability arising from seepage and pollution unless caused by a sudden, unintended and unexpected occurrence.

8 Maximum deductible threshold

8.1 Not to exceed [redacted] for each and every third party property damage claim (personal injury claims to be paid in full).

PART C: UNITED KINGDOM COMPULSORY INSURANCES

1 UNITED KINGDOM COMPULSORY INSURANCES

1.1 The Supplier shall meet its insurance obligations under applicable Law in full, including, UK employers' liability insurance and motor third party liability insurance.

1.2 The limit of indemnity for the employers' liability insurance shall not be less than [redacted] (or such other limit as may be required by Law from time to time) for any one occurrence inclusive of costs.

1.3 The employers' liability insurance shall contain an indemnity to principals clause under which the Authority shall be indemnified in respect of claims made against the Authority arising from the acts or omissions or the performance by the Supplier of the Services and in connection with this Agreement.

PART D: ADDITIONAL INSURANCES

1 Professional Indemnity Insurance

1.1 **Insured**

The Supplier (the "**Insured**")

1.2 **Interest**

To indemnify the Insured for all sums which the Insured shall become legally liable to pay (including claimants costs and expenses) as a result of claims first made against the Insured during the period of Insurance by reason of any negligent act, error and/or omission arising from or in connection with the provision of the Services and in connection with this Agreement.

1.3 **Limit of Indemnity**

Not less than [redacted] in respect of any one claim and in the aggregate per annum.

1.4 **Territorial Limits**

United Kingdom

1.5 **Period of Insurance**

From the date of this Agreement for the duration of this Agreement and renewable on an annual basis unless agreed otherwise and a period of three years (3) following the expiry date or the termination date whichever occurs earlier.

1.6 **Cover Features and Extensions**

Retroactive cover to apply to any claims made policy wording in respect of the Agreement or retroactive date to be no later than the date of this Agreement.

1.7 **Principal Exclusions**

War and related perils

Nuclear and radioactive risks

1.8 **Maximum Deductible**

Not to exceed [redacted] for each and every claim

MODEL AGREEMENT FOR SERVICES SCHEDULES

SCHEDULE 3

AUTHORITY RESPONSIBILITIES

Authority Responsibilities

1 INTRODUCTION

1.1 The responsibilities of the Authority set out in this Schedule shall constitute the Authority Responsibilities under this Agreement. Any obligations of the Authority in Schedule 2 (*Services Description*) and Schedule 4 (*Supplier Solution*) shall not be Authority Responsibilities and the Authority shall have no obligation to perform any such obligations unless they are specifically stated to be "Authority Responsibilities".

1.2 The responsibilities specified within this Schedule shall be provided to the Supplier free of charge, unless otherwise agreed between the Parties.

2 GENERAL OBLIGATIONS

2.1 The Authority shall:

(a) perform those obligations of the Authority which are set out in the Clauses of this Agreement and the Paragraphs of the Schedules (except Schedule 2 (*Services Description*) and Schedule 4 (*Supplier Solution*));

(b) use its reasonable endeavours to provide the Supplier with access to appropriate members of the Authority's staff, as such access is reasonably requested by the Supplier in order for the Supplier to discharge its obligations throughout the Term and the Termination Assistance Period;

(c) provide sufficient and suitably qualified staff to fulfil the Authority's roles and duties under this Agreement; and

(d) use its reasonable endeavours to provide such documentation, data and/or other information that the Supplier reasonably requests that is necessary to perform its obligations under the terms of this Agreement provided that such documentation, data and/or information is available to the Authority and is authorised for release by the Authority;

3 NOT USED

[redacted]

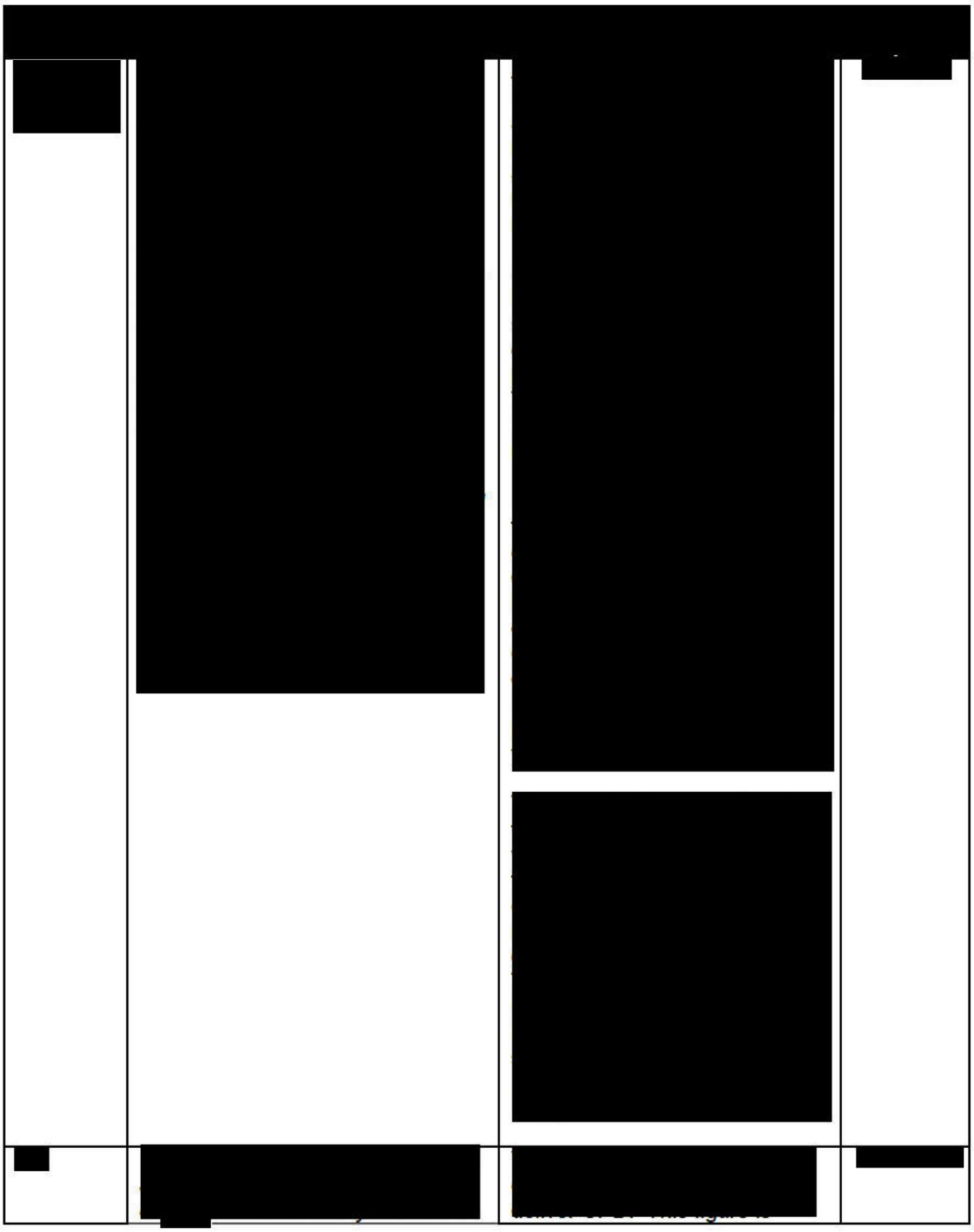
[redacted]

[redacted]

[redacted]

[redacted]

[redacted]



[redacted]