

CONTRACT FOR JOURNALS ACCESS

THIS CONTRACT IS DATED 23/04/2020

Parties

- 1) The Secretary of State for Education whose Head Office is at Sanctuary Buildings, Great Smith Street, London, SW1P 3BT acting as part of the Crown (“the Department”); and
- 2) EBSCO Information Services BR011966 whose registered office is at 6th Floor, Civic Centre Silver Street, Enfield, EN1 3XA (“the Contractor”)

Recitals

The Contractor has agreed to provide access to academic Journals through a ‘one stop shop’ portal based approach on the terms and conditions set out in this Contract.

The Department's reference number for this Contract is project_1073.

1 Interpretation

1.1 In this Contract the following words shall mean:-

“the Services”	the services to be performed by the Contractor as described in Schedule 1;
"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;
“Central Government Body”	means 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;

"the Contract Manager"

Robin Elliott Marshall

1st Floor, 2 St Paul's Place, 125 Norfolk St,
Sheffield S1 2FJ

"Contract Period"

The start and end date of the contract as set out in Clause 2 subject to any extensions.

"Contractor Personnel"

all employees, agents, Contractors and contractors of the Contractor and/or of any Sub-contractor;

"the Contractors Contract Manager"

*** TBC***

"Confidential Information"

the Department's Confidential Information and/or the Contractor's Confidential Information;

"Contracting Department"

any contracting Department as defined in Regulation 5(2) of the Public Contracts (Works, Services and Supply) (Amendment) Regulations 2000 other than the Department;

"Contractor Personnel"

all employees, agents, consultants and contractors of the Contractor and/or of any Sub-contractor;

"Contracts Finder"

the Government's publishing portal for public sector procurement

opportunities.

"Control"

means that a person possesses, directly or indirectly, 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”, “Processor”, “Data Subject”, “Personal Data”, “Personal Data Breach”, “Data Protection Officer”	take the meaning given in the GDPR
“Crown”	means Queen Elizabeth II and any successor
"Crown Body"	any department, office or agency of the Crown;
“Data Loss Event”	any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach.
“DPA 2018”	Data Protection Act 2018
“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”	(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy;
“Data 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 access their Personal Data.
"Department's Confidential Information"	all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel, and suppliers of the Department, including all IPRs, together with all information derived from any of the above, and any other information clearly designated as being confidential (whether or not it is marked

	"confidential") or which ought reasonably be considered to be confidential;
"Department's Intellectual Property Rights"	means all Intellectual Property Rights comprised in or necessary for or arising from the performance of the Consultancy Services
"Environmental Information Regulations"	the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government Department in relation to such regulations;
"FOIA"	the Freedom of Information Act 2000 and any subordinate legislation made under this Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government Department in relation to such legislation;
"GDPR"	the General Data Protection Regulation (Regulation (EU) 2016/679)
"Her Majesty's Government"	means the duly elected Government for the time being during the reign of Her Majesty and/or any department, committee, office, servant or officer of such Government
"Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;
"Intellectual Property Rights"	means any copyright, rights in designs, database rights, domain names, trade marks, service marks, patents or any applications for any of the foregoing, know-how or similar rights or obligations (whether registerable or not) including Moral Rights as defined in Chapter IV of the Copyright, Designs and Patents Act 1988
"Joint Controllers"	Where two or more Controllers jointly determine the purposes and means of processing
"Law"	means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable

	right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Processor is bound to comply;
"LED"	Law Enforcement Directive (Directive (EU) 2016/680)
"Personal Data"	shall have the same meaning as set out in the Data Protection Act 1998;
"Processor Personnel"	employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Contract.
"Property"	means the property, other than real property, issued or made available to the Contractor by the Client in connection with the Contract.
"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 including those set out in the Contract. .
"Regulatory Bodies"	those government departments and regulatory, statutory and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this Contract or any other affairs of the Department and " Regulatory Body " shall be construed accordingly.
"Request for Information"	a request for information or an apparent request under the Code of Practice on Access to

	Government Information, FOIA or the Environmental Information Regulations;
"SME"	means a micro, small or medium-sized enterprise defined in accordance with the European Commission Recommendation 2003/361/EC and any subsequent revisions.
"Sub-contractor"	the third party with whom the Contractor enters into a Sub-contract or its servants or agents and any third party with whom that third party enters into a Sub-contract or its servants or agents;
"Sub-processor"	any third Party appointed to process Personal Data on behalf of the Contractor related to this Contract
"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.

- 1.2** References to "Contract" mean this contract (and include the Schedules). References to "Clauses" and "Schedules" mean clauses of and schedules to this Contract. The provisions of the Schedules shall be binding on the parties as if set out in full in this Contract.
- 1.3** Reference to the singular include the plural and vice versa and references to any gender include both genders and the neuter. References to a person include any individual, firm, unincorporated association or body corporate.

2 Commencement and Continuation

The Contractor shall commence the Services on 23/04/2020 and, subject to Clause 10.1 shall complete the Services on or before 31/03/2022.

The contract may be extended by up to 12 months subject to satisfactory performance.

3 Contractor's Obligations

- 3.1** The Contractor shall promptly and efficiently complete the Services in accordance with the provisions set out in Schedule 1 and the special conditions set out in

Schedule 3. Where there is any conflict between the terms of this Contract and the special conditions set out in Schedule 3, the special conditions shall prevail.

- 3.2 The Contractor shall comply with the accounting and information provisions of Schedule 2.
- 3.3 The Contractor shall comply with all statutory provisions including all prior and subsequent enactments, amendments and substitutions relating to that provision and to any regulations made under it.

4 Departments Obligations

The Department will comply with the payment provisions of Schedule 2 provided that the Department has received full and accurate information and documentation as required by Schedule 2 to be submitted by the Contractor for work completed to the satisfaction of the Department.

5 Changes to the Department's Requirements

- 5.1 The Department shall notify the Contractor of any material change to the Department's requirement under this Contract.
- 5.2 The Contractor shall use its best endeavours to accommodate any changes to the needs and requirements of the Department provided that it shall be entitled to payment for any additional costs it incurs as a result of any such changes. The amount of such additional costs to be agreed between the parties in writing.

6 Management

- 6.1 The Contractor shall promptly comply with all reasonable requests or directions of the Contract Manager in respect of the Services.
- 6.2 The Contractor shall address any enquiries about procedural or contractual matters in writing to the Contract Manager. Any correspondence relating to this Contract shall quote the reference number set out in the Recitals to this Contract.

7 Contractor's Employees and Sub-Contractors

- 7.1 Where the Contractor enters into a contract with a supplier or contractor for the purpose of performing its obligations under the Contract (the "**Sub-contractor**") it shall ensure prompt payment in accordance with this clause 7.1. Unless otherwise agreed by the Department in writing, the Contractor shall ensure that any contract requiring payment to a Sub-contractor shall provide for undisputed sums due to the Sub-contractor to be made within a specified period from the receipt of a valid invoice not exceeding:

7.1.1 10 days, where the Sub-contractor is an SME; or

7.1.2 30 days either, where the sub-contractor is not an SME, or both the Contractor and the Sub-contractor are SMEs,

The Contractor shall comply with such terms and shall provide, at the Department's request, sufficient evidence to demonstrate compliance.

- 7.2** The Department shall be entitled to withhold payment due under clause 7.1 for so long as the Contractor, in the Department's reasonable opinion, has failed to comply with its obligations to pay any Sub-contractors promptly in accordance with clause 7.1. For the avoidance of doubt the Department shall not be liable to pay any interest or penalty in withholding such payment. .
- 7.3** The Contractor shall take all reasonable steps to satisfy itself that its employees or sub-contractors (or their employees) are suitable in all respects to perform the Services.
- 7.4** The Contractor shall give to the Department if so requested a list of all persons who are or may be at any time directly concerned with the performance of this Contract specifying the capacity in which they are concerned with the provision of the Services and giving such other particulars as the Department may reasonably require.
- 7.5** If the Department notifies the Contractor that it considers that an employee or sub-contractor is not appropriately qualified or trained to provide the Services or otherwise is not providing the Services in accordance with this Contract, then the Contractor shall, as soon as is reasonably practicable, take all such steps as the Department considers necessary to remedy the situation or, if so required by the Department, shall remove the said employee or sub-contractor from providing the Services and shall provide a suitable replacement (at no cost to the Department).
- 7.6** The Contractor shall take all reasonable steps to avoid changes of employees or sub-contractors assigned to and accepted to provide the Services under the Contract except whenever changes are unavoidable or of a temporary nature. The Contractor shall give at least one month's written notice to the Contract Manager of proposals to change key employees or sub-contractors.
- 7.7** The Contractor shall immediately notify the Department if they have any concerns regarding the propriety of any of its sub-contractors in respect of work/services rendered in connection with this Contract.
- 7.8** The Contractor, its employees and sub-contractors (or their employees), whilst on Departmental premises, shall comply with such rules, regulations and requirements (including those relating to security arrangements) as may be in force from time to time.
- 7.9** The Contractor shall ensure the security of all the Property whilst in its possession, during the supply of the Services, in accordance with the Department's reasonable security requirements as required from time to time.

7.10 The Contractor shall:

- 7.10.1 subject to clause 7.10.7, advertise on Contracts Finder all subcontract opportunities arising from or in connection with the provision of the Services above a minimum threshold of £25,000 that arise during the Contract Period;
- 7.10.2 within 90 days of awarding a subcontract to a subcontractor, update the notice on Contracts Finder with details of the successful subcontractor;
- 7.10.3 monitor the number, type and value of the subcontract opportunities placed on Contracts Finder advertised and awarded in its supply chain during the Contract Period;
- 7.10.4 provide reports on the information at clause 7.10.3 to the Department in the format and frequency as reasonably specified by the Department;
- 7.10.5 promote Contracts Finder to its suppliers and encourage those organisations to register on Contracts Finder.
- 7.10.6 Each advert referred to at clause 7.10.1 above shall provide a full and detailed description of the subcontract opportunity with each of the mandatory fields being completed on Contracts Finder by the Contractor.
- 7.10.7 The obligation at Clause 7.10.1 shall only apply in respect of subcontract opportunities arising after the contract award date.
- 7.10.8 Notwithstanding clause 7.10, the Department may by giving its prior written approval, agree that a subcontract opportunity is not required to be advertised on Contracts Finder.

7.11 In addition to any other management information requirements set out in this Contract, the Contractor agrees and acknowledges that it shall, on request and at no charge, provide timely, full, accurate and complete SME Management Information (MI) Reports to the Department including:

- 7.11.1 the total contract revenue received directly on a specific contract;
- 7.11.2 the total value of sub-contracted revenues under the contract (including revenues for non-SMEs/non-VCSEs); and
- 7.11.3 the total value of sub-contracted revenues to SMEs and VCSEs.

8 Intellectual Property Rights

- 8.1** It is acknowledged and agreed between the parties that all existing or future Department's Intellectual Property Rights shall vest in the Crown absolutely.
- 8.2** The Contractor agrees that at the request and cost of the Department it will and procure that its officers, employees and agents will at all times do all such reasonable acts and execute all such documents as may be reasonably necessary

or desirable to ensure that the Department receives the full benefit of all of its rights under this Contract in respect of the Department's Intellectual Property Rights or to assist in the resolution of any question concerning the Intellectual Property Rights.

9 Warranty and Indemnity

- 9.1** The Contractor warrants to the Department that the obligations of the Contractor under this Contract will be performed by appropriately qualified and trained personnel with reasonable skill, care and diligence and to such high standards of quality as it is reasonable for the Department to expect in all the circumstances. The Department will be relying upon the Contractor's skill, expertise and experience in the performance of the Services and also upon the accuracy of all representations or statements made and the advice given by the Contractor in connection with the performance of the Services and the accuracy of any documents conceived, originated, made or developed by the Contractor as part of this Contract. The Contractor warrants that any goods supplied by the Contractor forming a part of the Services will be of satisfactory quality and fit for their purpose and will be free from defects in design, material and workmanship.
- 9.2** Without prejudice to any other remedy, if any part of the Services is not performed in accordance with this Contract then the Department shall be entitled, where appropriate to:
- 9.2.1 require the Contractor promptly to re-perform or replace the relevant part of the Services without additional charge to the Department; or
- 9.2.2 assess the cost of remedying the failure ("the assessed cost") and to deduct from any sums due to the Contractor the Assessed Cost for the period that such failure continues.
- 9.3** The Contractor shall be liable for and shall indemnify the Department in full against any expense, liability, loss, claim or proceedings arising under statute or at common law in respect of personal injury to or death of any person whomsoever or loss of or damage to property whether belonging to the Department or otherwise arising out of or in the course of or caused by the provision of the Services.
- 9.4** The Contractor shall be liable for and shall indemnify the Department against any expense, liability, loss, claim or proceedings arising as a result of or in connection with any breach of the terms of this Contract or otherwise through the default of the Contractor. Liability shall align to the terms outlined in Annex D – Licensing Agreement (Part II)
- 9.5** All property of the Contractor whilst on the Department's premises shall be there at the risk of the Contractor and the Department shall accept no liability for any loss or damage howsoever occurring to it.
- 9.6** The Contractor shall ensure that it has adequate insurance cover with an insurer of good repute to cover claims under this Contract or any other claims or demands which may be brought or made against it by any person suffering any injury damage

or loss in connection with this Contract. The Contractor shall upon request produce to the Department, its policy or policies of insurance, together with the receipt for the payment of the last premium in respect of each policy or produce documentary evidence that the policy or policies are properly maintained.

10 Termination

- 10.1** This Contract may be terminated by either party giving to the other party at least 3 months notice in writing.
- 10.2** In the event of any breach of this Contract by either party, the other party may serve a notice on the party in breach requiring the breach to be remedied within a period specified in the notice which shall be reasonable in all the circumstances. If the breach has not been remedied by the expiry of the specified period, the party not in breach may terminate this Contract with immediate effect by notice in writing.
- 10.3** In the event of a material breach of this Contract by either party, the other party may terminate this Contract with immediate effect by notice in writing.
- 10.4** This Contract may be terminated by the Department with immediate effect by notice in writing if at any time:-
- 10.4.1** the Contractor passes a resolution that it be wound-up or that an application be made for an administration order or the Contractor applies to enter into a voluntary arrangement with its creditors; or
 - 10.4.2** a receiver, liquidator, administrator, supervisor or administrative receiver be appointed in respect of the Contractor's property, assets or any part thereof; or
 - 10.4.3** the court orders that the Contractor be wound-up or a receiver of all or any part of the Contractor's assets be appointed; or
 - 10.4.4** the Contractor is unable to pay its debts in accordance with Section 123 of the Insolvency Act 1986.
 - 10.4.5** there is a change in the legal or beneficial ownership of 50% or more of the Contractor's share capital issued at the date of this Contract or there is a change in the control of the Contractor, unless the Contractor has previously notified the Department in writing. For the purpose of this Sub-Clause 10.4.5 "control" means the power of a person to secure that the affairs of the Contractor are conducted in accordance with the wishes of that person by means of the holding of shares or the possession of voting power.
 - 10.4.6** the Contractor is convicted (or being a company, any officers or representatives of the Contractor are convicted) of a criminal offence related to the business or professional conduct

10.4.7 the Contractor commits (or being a company, any officers or representatives of the Contractor commit) an act of grave misconduct in the course of the business;

10.4.8 the Contractor fails (or being a company, any officers or representatives of the Contractor fail) to fulfil its obligations relating to the payment of Social Security contributions;

10.4.9 the Contractor fails (or being a company, any officers or representatives of the Contractor fail) to fulfil its obligations relating to payment of taxes;

10.4.10 the Contractor fails (or being a company, any officers or representatives of the Contractor fail) to disclose any serious misrepresentation in supplying information required by the Department in or pursuant to this Contract.

10.5 Nothing in this Clause 10 shall affect the coming into, or continuance in force of any provision of this Contract which is expressly or by implication intended to come into force or continue in force upon termination of this Contract.

11 Status of Contractor

11.1 In carrying out its obligations under this Contract the Contractor agrees that it will be acting as principal and not as the agent of the Department.

11.2 The Contractor shall not say or do anything that may lead any other person to believe that the Contractor is acting as the agent of the Department.

12 Confidentiality

12.1 Except to the extent set out in this clause or where disclosure is expressly permitted elsewhere in this Contract, each party shall:

12.1.1 treat the other party's Confidential Information as confidential and safeguard it accordingly; and

12.1.2 not disclose the other party's Confidential Information to any other person without the owner's prior written consent.

12.2 Clause 12 shall not apply to the extent that:

12.2.1 such disclosure is a requirement of Law placed upon the party making the disclosure, including any requirements for disclosure under the FOIA, Code of Practice on Access to Government Information or the Environmental Information Regulations pursuant to Clause 13 (Freedom of Information);

- 12.2.2 such information was in the possession of the party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner;
 - 12.2.3 such information was obtained from a third party without obligation of confidentiality;
 - 12.2.4 such information was already in the public domain at the time of disclosure otherwise than by a breach of this Contract; or
 - 12.2.5 it is independently developed without access to the other party's Confidential Information.
- 12.3** The Contractor may only disclose the Department's Confidential Information to the Contractor Personnel who are directly involved in the provision of the Project and who need to know the information, and shall ensure that such Contractor Personnel are aware of and shall comply with these obligations as to confidentiality.
- 12.4** The Contractor shall not, and shall procure that the Contractor Personnel do not, use any of the Department's Confidential Information received otherwise than for the purposes of this Contract.
- 12.5** The Contractor shall ensure that their employees, servants or such professional advisors or consultants are aware of the Contractor's obligations under this Contract.
- 12.6** Nothing in this Contract shall prevent the Department from disclosing the Contractor's Confidential Information:
- 12.6.1 on a confidential basis to any Central Government Body for any proper purpose of the Department or of the relevant Central Government Body;
 - 12.6.2 to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement;
 - 12.6.3 on a confidential basis to a professional adviser, consultant, supplier or other person engaged by any of the entities described in Clause 12.6.1 (including any benchmarking organisation) for any purpose relating to or connected with this Contract;
 - 12.6.4 on a confidential basis for the purpose of the exercise of its rights under this Contract, including audit rights, step-in rights and exit management rights; or
 - 12.6.5 on a confidential basis to a proposed successor body in connection with any assignment, novation or disposal of any of its rights, obligations or liabilities under this Contract.
- 12.7** The Department shall use all reasonable endeavours to ensure that any Central Government Body, Contracting Department, employee, third party or Sub-contractor to whom the Contractor's Confidential Information is disclosed pursuant to clause 12 is made aware of the Department's obligations of confidentiality.

- 12.8** Nothing in this clause 12 shall prevent either party from using any techniques, ideas or know-how gained during the performance of the Contract in the course of its normal business to the extent that this use does not result in a disclosure of the other party's Confidential Information or an infringement of Intellectual Property Rights.
- 12.9** The parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of this Contract is not Confidential Information. The Department shall be responsible for determining in its absolute discretion whether any of the content of the Contract is exempt from disclosure in accordance with the provisions of the FOIA.
- 12.10** Subject to Clause 12.9, the Contractor hereby gives its consent for the Department to publish the Contract in its entirety, including from time to time agreed changes to the Contract, to the general public.
- 12.11** The Department may consult with the Contractor to inform its decision regarding any redactions but the Department shall have the final decision in its absolute discretion.
- 12.12** The Contractor shall assist and cooperate with the Department to enable the Department to publish this Contract.

13 Freedom of Information

- 13.1** The Contractor acknowledges that the Department is subject to the requirements of the FOIA and the Environmental Information Regulations and shall assist and cooperate with the Department to enable the Department to comply with its information disclosure obligations.
- 13.2** The Contractor shall:
- 13.2.1 transfer to the Department all Requests for Information that it receives as soon as practicable and in any event within two Working Days of receiving a Request for Information;
 - 13.2.2 provide the Department with a copy of all Information in its possession, or power in the form that the Department requires within five Working Days (or such other period as the Department may specify) of the Department's request; and
 - 13.2.3 provide all necessary assistance as reasonably requested by the Department to enable the Department to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations.
- 13.3** The Department shall be responsible for determining in its absolute discretion and notwithstanding any other provision in this Contract or any other agreement whether

any Information is exempt from disclosure in accordance with the provisions of the FOIA or the Environmental Information Regulations.

13.4 In no event shall the Contractor respond directly to a Request for Information unless expressly authorised to do so by the Department.

13.5 The Contractor acknowledges that (notwithstanding the provisions of Clause 13) the Department may, acting in accordance with the Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000 ("**the Code**"), be obliged under the FOIA, or the Environmental Information Regulations to disclose information concerning the Contractor or the Project:

13.5.1 in certain circumstances without consulting the Contractor; or

13.5.2 following consultation with the Contractor and having taken their views into account;

provided always that where 13.5.1 applies the Department shall, in accordance with any recommendations of the Code, take reasonable steps, where appropriate, to give the Contractor advanced notice, or failing that, to draw the disclosure to the Contractor's attention after any such disclosure.

13.6 The Contractor shall ensure that all Information is retained for disclosure and shall permit the Department to inspect such records as requested from time to time.

14 Access and Information

The Contractor shall provide access at all reasonable times to the Department's internal auditors or other duly authorised staff or agents to inspect such documents as the Department considers necessary in connection with this Contract and where appropriate speak to the Contractors employees.

15 Transfer of Responsibility on Expiry or Termination

15.1 The Contractor shall, at no cost to the Department, promptly provide such assistance and comply with such timetable as the Department may reasonably require for the purpose of ensuring an orderly transfer of responsibility upon the expiry or other termination of this Contract. The Department shall be entitled to require the provision of such assistance both prior to and, for a reasonable period of time after the expiry or other termination of this Contract.

15.2 Such assistance may include (without limitation) the delivery of documents and data in the possession or control of the Contractor which relate to this Contract, including the documents and data, if any, referred to in the Schedule.

15.3 The Contractor undertakes that it shall not knowingly do or omit to do anything which may adversely affect the ability of the Department to ensure an orderly transfer of responsibility.



16 Tax Indemnity

- 16.1** Where the Contractor is liable to be taxed in the UK in respect of consideration received under this contract, it shall at all times comply with the Income Tax (Earnings and Pensions) Act 2003 (ITEPA) and all other statutes and regulations relating to income tax in respect of that consideration. Where the Department has deemed the Contractor to be an Off-Payroll Contractor as defined by Her Majesty's Revenue and Customs the Department reserves the right to calculate Income Tax and pay it to HMRC. The amounts will be deducted from the Contractor's fee for the work provided.
- 16.2** Where the Contractor is liable to National Insurance Contributions (NICs) in respect of consideration received under this contract, it shall at all times comply with the Social Security Contributions and Benefits Act 1992 (SSCBA) and all other statutes and regulations relating to NICs in respect of that consideration. . Where the Department has deemed the Contractor to be an Off-Payroll Contractor as defined by Her Majesty's Revenue and Customs the Department reserves the right to calculate primary (employee) National Insurance contributions (NICs) and pay them to HMRC. The amounts will be deducted from the Contractor's fee for the work provided.
- 16.3** The Department may, at any time during the term of this contract, ask the Contractor to provide information which demonstrates how the Contractor complies with Clauses 16.1 and 16.2 above or why those Clauses do not apply to it.
- 16.4** A request under Clause 16.3 above may specify the information which the Contractor must provide and the period within which that information must be provided.
- 16.5** The Department may terminate this contract if-
- (a) in the case of a request mentioned in Clause 16.3 above if the Contractor:
 - (i) fails to provide information in response to the request within a reasonable time,or
 - (ii) provides information which is inadequate to demonstrate either how the Contractor complies with Clauses 16.1 and 16.2 above or why those Clauses do not apply to it;
 - (b) in the case of a request mentioned in Clause 16.4 above, the Contractor fails to provide the specified information within the specified period, or
 - (c) it receives information which demonstrates that, at any time when Clauses 16.1 and 16.2 apply, the Contractor is not complying with those Clauses.
- 16.6** The Department may supply any information which it receives under Clause 16.3 to the Commissioners of Her Majesty's Revenue and Customs for the purpose of the collection and management of revenue for which they are responsible.

- 16.7** The Contractor warrants and represents to the Department that it is an independent contractor and, as such, bears sole responsibility for the payment of tax and national insurance contributions which may be found due from it in relation to any payments or arrangements made under this Contract or in relation to any payments made by the Contractor to its officers or employees in connection with this Contract.
- 16.8** The Contractor will account to the appropriate authorities for any income tax, national insurance, VAT and all other taxes, liabilities, charges and duties relating to any payments made to the Contractor under this Contract or in relation to any payments made by the Contractor to its officers or employees in connection with this Contract.
- 16.9** The Contractor shall indemnify Department against any liability, assessment or claim made by the HM Revenue and Customs or any other relevant authority arising out of the performance by the parties of their obligations under this Contract (other than in respect of employer's secondary national insurance contributions) and any costs, expenses, penalty fine or interest incurred or payable by Department in connection with any such assessment or claim.
- 16.10** The Contractor authorises the Department to provide the HM Revenue and Customs and all other departments or agencies of the Government with any information which they may request as to fees and/or expenses paid or due to be paid under this Contract whether or not Department is obliged as a matter of law to comply with such request.

17 Data Protection

- 17.1** The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor unless otherwise specified in Schedule 3a. The only processing that the Processor is authorised to do is listed in Schedule 3a by the Controller and may not be determined by the Processor
- 17.2** The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.
- 17.3** The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:
- (a) a systematic description of the envisaged processing operations and the purpose of the processing;
 - (b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;
 - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
 - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

17.4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Contract:

- (a) process that Personal Data only in accordance with Schedule 3a , unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;
- (b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Data Loss Event;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
- (c) ensure that :
 - (i) the Processor Personnel do not process Personal Data except in accordance with this Contract (and in particular Schedule 3a);
 - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (A) are aware of and comply with the Processor's duties under this clause;
 - (B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
 - (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Contract; and
 - (D) have undergone adequate training in the use, care, protection and handling of Personal Data; and
- (d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
 - (i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;
 - (ii) the Data Subject has enforceable rights and effective legal remedies;
 - (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
 - (iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

- (e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

17.5 Subject to clause 17.6, the Processor shall notify the Controller immediately if it:

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

17.6 The Processor's obligation to notify under clause 17.5 shall include the provision of further information to the Controller in phases, as details become available.

17.7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 17.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

- (a) the Controller with full details and copies of the complaint, communication or request;
- (b) such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;
- (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
- (d) assistance as requested by the Controller following any Data Loss Event;
- (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

17.8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

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



- 17.9** The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
- 17.10** Each Party shall designate its own data protection officer if required by the Data Protection Legislation.
- 17.11** Before allowing any Sub-processor to process any Personal Data related to this Contract, the Processor must:
- (a) notify the Controller in writing of the intended Sub-processor and processing;
 - (b) obtain the written consent of the Controller;
 - (c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause 17 such that they apply to the Sub-processor; and
 - (d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.
- 17.12** The Processor shall remain fully liable for all acts or omissions of any Sub-processor.
- 17.13** The Controller may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Contract).
- 17.14** The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

18 Amendment and variation

No amendment or variation to this Contract shall be effective unless it is in writing and signed by or on behalf of each of the parties hereto. The Contractor shall comply with any formal procedures for amending or varying contracts which the Department may have in place from time to time.

19 Assignment and Sub-contracting

The benefit and burden of this Contract may not be assigned or sub-contracted in whole or in part by the Contractor without the prior written consent of the Department. Such consent may be given subject to any conditions which the Department considers necessary. The Department may withdraw its consent to any sub-contractor where it no longer has reasonable grounds to approve of the sub-contractor or the sub-contracting arrangement and where these grounds have been presented in writing to the Contractor.

20 The Contract (Rights of Third Parties) Act 1999

This Contract is not intended to create any benefit, claim or rights of any kind whatsoever enforceable by any person not a party to the Contract.

21 Waiver

No delay by or omission by either Party in exercising any right, power, privilege or remedy under this Contract shall operate to impair such right, power, privilege or remedy or be construed as a waiver thereof. Any single or partial exercise of any such right, power, privilege or remedy shall not preclude any other or further exercise thereof or the exercise of any other right, power, privilege or remedy.

22 Notices

22.1 Any notice, demand or communication in connection with the Contract shall be in writing and may be delivered by hand, pre-paid first class post or (where being sent to an address in a different country to where posted) airmail, or e-mail, addressed to the recipient at its registered office or its address (or such other address, or e-mail address as may be notified in writing from time to time).

22.2 The notice, demand or communication shall be deemed to have been duly served:

22.2.1 if delivered by hand, when left at the proper address for service;

22.2.2 if given or made by prepaid first class post 48 hours after being posted or in the case of airmail 14 days after being posted;

22.2.3 if made by e-mail, at the time of transmission, dispatched as a pdf attachment to an e-mail to the correct e-mail address without any error message or, in the case of transmission by e-mail where the time of transmission is not between 9.00 am and 5.00 pm, service shall be deemed to occur at 9.00 am on the next following Business Day (such times being local time at the address of the recipient).

23 Dispute resolution

23.1 The Parties shall use all reasonable endeavours to negotiate in good faith and settle amicably any dispute that arises during the continuance of this Contract.

23.2 Any dispute not capable of resolution by the parties in accordance with the terms of Clause 23 shall be settled as far as possible by mediation in accordance with the Centre for Dispute Resolution (CEDR) Model Mediation Procedure.

23.3 No party may commence any court proceedings/arbitration in relation to any dispute arising out of this Contract until they have attempted to settle it by mediation, but any such mediation may be terminated by either party at any time of such party wishing to commence court proceedings/arbitration.

24 Discrimination



- 24.1** The Contractor shall not unlawfully discriminate within the meaning and scope of any law, enactment, order, or regulation relating to discrimination (whether in race, gender, religion, disability, sexual orientation or otherwise) in employment.
- 24.2** The Contractor shall take all reasonable steps to secure the observance of Clause 24.1 by all servants, employees or agents of the Contractor and all suppliers and sub-contractors employed in the execution of the Contract.

25 Law and Jurisdiction

This Contract shall be governed by and interpreted in accordance with English Law and the parties submit to the jurisdiction of the English courts.

As witness the hands of the parties

Authorised to sign for and on
behalf of the Secretary of

State for Education



Authorised to sign for and on
behalf of EBSCO Information
Services



Schedule 1: Schedule of Work

Schedule 1

1 Background

- 1.1 The DfE is responsible for children's services and education, including early years, schools, higher and further education policy, apprenticeships and wider skills in England. It has around 5,200 staff and a budget of £64bn in 2019-20, although the bulk of this is then allocated by DfE to other bodies (e.g. £47.6bn for schools). The DfE spends around £29m a year on research and development. However we also need to learn from research from other organisations, both in the UK and internationally. Most high-quality scientific research funded outside government is published through academic journals. DfE needs access to as much relevant research evidence as possible to ensure that our advice to ministers and internal policy and delivery decisions are informed by the latest insight and evidence available. Advice is often needed quickly (sometimes within 24 hours), so we cannot wait for print copies or arranging access to specific articles. To help ensure our advice draws on the latest and most relevant research evidence we need readily available electronic access at our fingertips to as much relevant full text, UK and international English language publication as feasible.

2 Aim

- 2.1 The Contractor shall use all reasonable endeavours to achieve the following aims:
- Significant improvement of the access and coverage of academic journals available to the Department for Education.
 - Increasing the visibility and usage of academic journals to inform research, policy and delivery decisions within the Department for Education.

3 Objectives

- 3.1 The Contractor shall use all reasonable endeavours to achieve the following objectives:
- Increase the levels of usage of academic journals through a centralised portal in the Department for Education.
 - Provide an effective service offering of academic content to serve the Department for Education's research, policy and delivery needs.
 - Collaborate with the Department to refine the service offering throughout the term of the contract.

4 Methodology

The Contractor shall perform the tasks detailed in the Schedule of Work.

SCHEDULE OF WORK

Task	Output	Date Required/Frequency
Introductory session and mobilisation plan	Following award of the contract, an introductory session between the Department and the Contractor will take place to discuss tasks required for effective contract mobilisation. The supplier should then detail a mobilisation plan, outlining and agreeing the key steps and timescales with the Department's contract manager.	W/C 20/04/2020
Availability of required content (collections)	The supplier will make required EBSCO collections available to the Department using the existing form of access.	22/04/2020
Availability of required content (individual journals)	The supplier will make individual journals required by the Department available.	Timescales to be agreed
Provision of marketing materials	The supplier will provide copies of their off the shelf marketing materials to the Department's Contract Manager to support the launch of the portal. If any bespoke material is required, this will be delivered within an agreed timescale.	30/04/2020
Identification of key individuals	The supplier will provide details of key contacts for the Department in managing the contract (this has been provided within the suppliers bid). This should include names, email addresses and contact numbers. Where there is any change in key personnel, this change should be communicated to the Department's Contract Manager as soon as possible.	22/04/2020
Technical implementation	The supplier will collaborate with the relevant colleagues from the Department's Data Digital and Technology Directorate (as indicated by the Contract Manager) to ensure effective	The supplier and Contract Manager will agree a period for technical implementation and provide a plan in



	technical implementation of the new solution within an agreed timescales. Implementation will align to the three stages outlined in the supplier's bid and will cover authentication, methods of access for users, security and document delivery process amongst other things.	writing detailing this by W/C 20/04/2020.
Administration Portal	The supplier must put in place an administration portal with access provided to identified users within the Department. Access and training should be provided before the new solution goes live.	22/04/2020
Solution available	The supplier will ensure the solution is available for users to access in line with an agreed launch date. The launch date should be agreed with the Contract Manager as part of the mobilisation plan.	The supplier and Contract Manager will agree a date for the new solution to be available for use. The existing access to content will remain available until this point.
Training sessions	The supplier shall schedule and deliver training sessions to the Department's end users to support the launch of the solution. The supplier should ensure signposting to the training available which will include Customised Training for the Department to launch the new service, Live Online Courses and On Demand Training.	Standard training offer to be available throughout the contract term. A timetable of bespoke training for Department staff will be agreed with the Contract Manager.
Guidance and support	The supplier will ensure the appropriate guidance and support required for end users is available via an appropriate method. This will include written guidance as well as a dedicated user support function.	Throughout the contract term
Technical support	DFE will be allocated a technical support for contact to support users with technical queries. Access will also be provided to EBSCO Connect to support users throughout the contract term.	25/04/2020



Account development planning	The supplier should engage with the Department on a quarterly basis as part of supplier performance sessions to identify areas where the Department can enhance its offering, focusing on additional content that can be of value to replace content that is not being used.	Quarterly in the second week of each month.
Supplier performance meetings	The supplier will attend a quarterly performance meeting to discuss performance of the contract and discuss options for continuous improvement throughout the contract term.	Quarterly in the second week of each month.
Management Information provision	<p>The supplier will provide detailed management information to the Department's contract manager on a monthly basis. The content and format will be agreed with the contract manager in advance and reviewed on a quarterly basis at supplier performance meetings to ensure it is fit for purpose. Reports provided may be:</p> <ul style="list-style-type: none">• Database Usage Reports, Interface Usage, Link Activity, Login Activity, Title Usage, Top Search Terms Reports, Statistical Usage Analytics reports which present graphical data, Database Usage Analytics, Interface Usage Analytics and Login Usage.	MI to be provided on the first week of each month.
User survey	The supplier will facilitate a user survey on a bi-annual basis.	Biannually, throughout the contract term.
RED integration	The supplier will agree with the Contract Manager a plan to integrate the supplier's offering with the Department's Research Evidence Directory (RED).	Timeline to be agreed during the contract term with the Contract Manager.

5 Service Level Agreements and Key Performance Indicators



Supplier performance should align to the service levels and key performance indicators outlined in Annex B – Statement of Requirements.

The Key Performance Indicators here will be used to measure supplier performance on a quarterly basis as part of quarterly supplier performance meetings.



Schedule 2

The total contract value is £172,796. The current payment schedule accounts for payments for EBSCO hosted content and professional services. Payments for third party content provided as part of the contract will be added to the payment schedule by contract variation once confirmed.

1 Table

Deliverables	Total	Invoice date
<p>Year 1 2020-2021:</p> <ul style="list-style-type: none"> • EBSCO Discovery Service Search Portal • EBSCO Single Sign On • Professional Services (2 days in first year) • British Education Index • Business Source Premier • Child Development & Adolescent Studies • EBSCO eBooks Education Subscription Collection • EBSCO eBooks for FE/HE Subscription Collection • EBSCO eBooks Psychology Subscription Collection • EconLit with Full Text • Education Source • ERIC • Family & Society Studies Worldwide • Political Science Complete • Psychology & Behavioral Sciences Collection • Social Sciences Full 	£66,000	31/04/2020



Text <ul style="list-style-type: none"> • Social Work Abstracts • Sociology Source Ultimate • UK & Ireland Reference Centre 		
Year 2 2021-2022: <ul style="list-style-type: none"> • EBSCO Discovery Service Search Portal • FE/HE eBook Collection <ul style="list-style-type: none"> • Education eBook Collection • Psychology eBook Collection • ERIC • British Education Index • Family & Society Studies Worldwide <ul style="list-style-type: none"> • Social Work Abstracts • Child Development & Adolescent Studies • UK & Ireland Reference Centre • Psychology & Behavioural Sciences Collection • Education Source (upgrade version to Education Research Complete) • Sociology Source Ultimate (upgrade version to SocINDEX with Full Text) <ul style="list-style-type: none"> • EconLit with Full Text • Political Science Complete <ul style="list-style-type: none"> • Social Sciences Full Text • Business Source Premier 	£65,000	01/04/2021
Total	£131,000	

- 2 The Contractor shall maintain full and accurate accounts for the Service against the expenditure headings in the Table. Such accounts shall be retained for at least 6 years after the end of the financial year in which the last payment was made under this Contract. Input and output VAT shall be included as separate items in such accounts.



- 3 The Contractor shall permit duly authorised staff or agents of the Department or the National Audit Office to examine the accounts at any reasonable time and shall furnish oral or written explanations of the account if required. The Department reserves the right to have such staff or agents carry out examinations into the economy, efficiency and effectiveness with which the Contractor has used the Department's resources in the performance of this Contract.
- 4 Invoices shall be prepared by the Contractor annually and shall be detailed against the expenditure headings set out in the Table. The Contractor or its nominated representative or accountant shall certify on the invoice that the amounts claimed were expended wholly and necessarily by the Contractor on the Service in accordance with the Contract and that the invoice does not include any costs being claimed from any other body or individual or from the Department within the terms of another contract.
- 5 The Department shall accept and process for payment an electronic invoice submitted for payment by the Contractor where the invoice is undisputed and where it complies with the standard on electronic invoicing. For the purposes of this paragraph, an electronic invoice complies with the standard on electronic invoicing where it complies with the European standard and any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870.
- 6 Invoices shall be sent, within 30 days of the end of the quarter to Department for Education PO Box 407 SSCL Phoenix House, Celtic Springs Bus. Park Newport NP10 8FZ, quoting the Contract reference number. The Department undertakes to pay correctly submitted invoices within 5 days of receipt. The Department is obliged to pay invoices within 30 days of receipt from the day of physical or electronic arrival at the nominated address of the Department. Any correctly submitted invoices that are not paid within 30 days will be subject to the provisions of the Late Payment of Commercial Debt (Interest) Act 1998. A correct invoice is one that: is delivered in timing in accordance with the contract; is for the correct sum; in respect of goods/services supplied or delivered to the required quality (or are expected to be at the required quality); includes the date, supplier name, contact details and bank details; quotes the relevant purchase order/contract reference and has been delivered to the nominated address. If any problems arise, contact the Department's Contract Manager. The Department aims to reply to complaints within 10 working days. The Department shall not be responsible for any delay in payment caused by incomplete or illegible invoices.
- 7 The Contractor shall have regard to the need for economy in all expenditure. Where any expenditure in an invoice, in the Department's reasonable opinion, is excessive having due regard to the purpose for which it was incurred, the Department shall only be liable to reimburse so much (if any) of the expenditure disallowed as, in the Department's reasonable opinion after consultation with the Contractor, would reasonably have been required for that purpose.



- 8 If this Contract is terminated by the Department due to the Contractors insolvency or default at any time before completion of the Service, the Department shall only be liable under paragraph 1 to reimburse eligible payments made by, or due to, the Contractor before the date of termination.
- 9 On completion of the Service or on termination of this Contract, the Contractor shall promptly draw-up a final invoice, which shall cover all outstanding expenditure incurred for the Service. The final invoice shall be submitted not later than 30 days after the date of completion of the Service.
- 10 The Department shall not be obliged to pay the final invoice until the Contractor has provided all the elements for each payment in Schedule 2.
- 11 It shall be the responsibility of the Contractor to ensure that the final invoice covers all outstanding expenditure for which reimbursement may be claimed. Provided that all previous invoices have been duly paid, on due payment of the final invoice by the Department all amounts due to be reimbursed under this Contract shall be deemed to have been paid and the Department shall have no further liability to make reimbursement of any kind.

End of Schedule 2

Schedule 3 – Special Conditions

Departmental Security Standards for Business Services and ICT Contracts

<p>“BPSS” “Baseline Personnel Security Standard”</p>	<p>a level of security clearance described as pre-employment checks in the National Vetting Policy. Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard</p>
<p>“CCSC” “Certified Cyber Security Consultancy”</p>	<p>is NCSC's approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. This approach builds on the strength of CLAS and certifies the competence of suppliers to deliver a wide and complex range of cyber security consultancy services to both the public and private sectors. See website: https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy</p>
<p>“CCP” “Certified Professional”</p>	<p>is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession and are building a community of recognised professionals in both the UK public and private sectors. See website: https://www.ncsc.gov.uk/scheme/certified-professional</p>
<p>“CC” “Common Criteria”</p>	<p>the Common Criteria scheme provides assurance that a developer's claims about the security features of their product are valid and have been independently tested against recognised criteria.</p>
<p>“CPA” “Commercial Product Assurance” [formerly called “CESG Product Assurance”]</p>	<p>is an ‘information assurance scheme’ which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards. These CPA certified products can be used by government, the wider public sector and industry. See website: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa</p>
<p>“Cyber Essentials” “Cyber Essentials Plus”</p>	<p>Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme.</p> <p>There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to one of these providers: https://www.iasme.co.uk/apply-for-self-assessment/</p>



<p>"Data"</p> <p>"Data Controller"</p> <p>"Data Processor"</p> <p>"Personal Data"</p> <p>"Sensitive Personal Data"</p> <p>"Data Subject", "Process" and "Processing"</p>	<p>shall have the meanings given to those terms by the Data Protection Act 2018</p>
<p>"Department's Data"</p> <p>"Department's Information"</p>	<p>is any data or information owned or retained in order to meet departmental business objectives and tasks, including:</p> <p>(a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are:</p> <p>(i) supplied to the Contractor by or on behalf of the Department; or</p> <p>(ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or</p> <p>(b) any Personal Data for which the Department is the Data Controller;</p>
<p>"DfE"</p> <p>"Department"</p>	<p>means the Department for Education</p>
<p>"Departmental Security Standards"</p>	<p>means the Department's security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver.</p>
<p>"Digital Marketplace / GCloud"</p>	<p>the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects. Cloud services (e.g. web hosting or IT health checks) are on the G-Cloud framework.</p>
<p>"FIPS 140-2"</p>	<p>this is the Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), entitled 'Security Requirements for Cryptographic Modules'. This document is the de facto security standard used for the accreditation of cryptographic modules.</p>
<p>"Good Industry Practice"</p> <p>"Industry Good Practice"</p>	<p>means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.</p>



<p>“Good Industry Standard”</p> <p>“Industry Good Standard”</p>	<p>means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.</p>
<p>“GSC”</p> <p>“GSCP”</p>	<p>means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications</p>
<p>“HMG”</p>	<p>means Her Majesty's Government</p>
<p>“ICT”</p>	<p>means Information and Communications Technology (ICT) is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution</p>
<p>“ISO/IEC 27001” “ISO 27001”</p>	<p>is the International Standard for Information Security Management Systems Requirements</p>
<p>“ISO/IEC 27002” “ISO 27002”</p>	<p>is the International Standard describing the Code of Practice for Information Security Controls.</p>
<p>“ISO 22301”</p>	<p>is the International Standard describing for Business Continuity</p>
<p>“IT Security Health Check (ITSHC)”</p> <p>“IT Health Check (ITHC)”</p> <p>“Penetration Testing”</p>	<p>means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.</p>
<p>“Need-to-Know”</p>	<p>the Need-to-Know principle is employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties.</p>
<p>“NCSC”</p>	<p>The National Cyber Security Centre (NCSC) formerly CESG is the UK government's National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk</p>
<p>“OFFICIAL”</p> <p>“OFFICIAL-SENSITIVE”</p>	<p>the term ‘OFFICIAL’ is used to describe the baseline level of ‘security classification’ described within the Government Security Classification Policy (GSCP) which details the level of protection to be afforded to information by HMG, for all routine public sector business, operations and services.</p> <p>the ‘OFFICIAL–SENSITIVE’ caveat is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the</p>



	media, as described in the Government Security Classification Policy.
"Secure Sanitisation"	<p>Secure sanitisation is the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. Some forms of sanitisation will allow you to re-use the media, while others are destructive in nature and render the media unusable. Secure sanitisation was previously covered by "Information Assurance Standard No. 5 - Secure Sanitisation" ("IS5") issued by the former CESG. Guidance can now be found at:</p> <p>https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media</p> <p>The disposal of physical documents and hardcopy materials advice can be found at:</p> <p>https://www.cpni.gov.uk/secure-destruction</p>
"Security and Information Risk Advisor" "CCP SIRA" "SIRA"	<p>the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also:</p> <p>https://www.ncsc.gov.uk/articles/about-certified-professional-scheme</p>
"SPF" "HMG Security Policy Framework"	<p>This is the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government's Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely.</p> <p>https://www.gov.uk/government/publications/security-policy-framework</p>
"Tailored Assurance" [formerly called "CTAS", or, "CESG Tailored Assurance"]	<p>is an 'information assurance scheme' which provides assurance for a wide range of HMG, MOD, Critical National Infrastructure (CNI) and public sector customers procuring IT systems, products and services, ranging from simple software components to national infrastructure networks.</p> <p>https://www.ncsc.gov.uk/documents/ctas-principles-and-methodology</p>



- 1.1. The Contractor shall comply with Departmental Security Standards for Contractors which include but are not constrained to the following clauses.
- 1.2. Where the Contractor will provide ICT products or services or otherwise handle information at OFFICIAL on behalf of the Department, the requirements under Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - [Action Note 09/14](#) 25 May 2016, or any subsequent updated document, are mandated; that “contractors supplying products or services to HMG shall have achieved, and retain certification at the appropriate level, under the HMG Cyber Essentials Scheme”. The certification scope must be relevant to the services supplied to, or on behalf of, the Department.
- 1.3 The Contractor shall be able to demonstrate conformance to, and show evidence of such conformance to the ISO/IEC 27001 (Information Security Management Systems Requirements) standard, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).
- 1.4 The Contractor shall follow the UK Government Security Classification Policy (GSCP) in respect of any Departmental Data being handled in the course of providing this service, and will handle this data in accordance with its security classification. (In the event where the Contractor has an existing Protective Marking Scheme then the Contractor may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Departmental Data).
- 1.5 Departmental Data being handled in the course of providing an ICT solution or service must be segregated from all other data on the Contractor’s or sub-contractor’s own IT equipment to protect the Departmental Data and enable the data to be identified and securely deleted when required. In the event that it is not possible to segregate any Departmental Data then the Contractor and any sub-contractor shall be required to ensure that it is stored in such a way that it is possible to securely delete the data in line with Clause 1.14.
- 1.6 The Contractor shall have in place and maintain physical security, in line with those outlined in ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access) to premises and sensitive areas
- 1.7 The Contractor shall have in place and maintain an access control policy and process for the logical access (e.g. identification and authentication) to ICT systems to ensure only authorised personnel have access to Departmental Data.
- 1.8 The Contractor shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to: physical security controls; good industry standard policies and process; anti-virus and firewalls; security updates and up-to-date patching regimes for anti-virus solutions; operating systems, network devices, and application software, user access controls and the creation and retention of audit logs of system use.



- 1.9 Any data in transit using either physical or electronic transfer methods across public space or cyberspace, including mail and couriers systems, or third party provider networks must be protected via encryption which has been certified to FIPS 140-2 standard or a similar method approved by the Department prior to being used for the transfer of any Departmental Data.
- 1.10 Storage of Departmental Data on any portable devices or media shall be limited to the absolute minimum required to deliver the stated business requirement and shall be subject to Clause 1.11 and 1.12 below.
- 1.11 Any portable removable media (including but not constrained to pen drives, flash drives, memory sticks, CDs, DVDs, or other devices) which handle, store or process Departmental Data to deliver and support the service, shall be under the control and configuration management of the contractor or (sub-)contractors providing the service, shall be both necessary to deliver the service and shall be encrypted using a product which has been certified to FIPS140-2 standard or another encryption standard that is acceptable to the Department.
- 1.12 All portable ICT devices, including but not limited to laptops, tablets, smartphones or other devices, such as smart watches, which handle, store or process Departmental Data to deliver and support the service, shall be under the control and configuration management of the contractor or sub-contractors providing the service, and shall be necessary to deliver the service. These devices shall be full-disk encrypted using a product which has been certified to FIPS140-2 standard or another encryption standard that is acceptable to the Department.
- 1.13 Whilst in the Contractor's care all removable media and hardcopy paper documents containing Departmental Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.
- 1.14 When necessary to hand carry removable media and/or hardcopy paper documents containing Departmental Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This clause shall apply equally regardless of whether the material is being carried inside or outside of company premises.
- 1.15 At the end of the contract or in the event of equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored on the Contractor's ICT infrastructure must be securely sanitised or destroyed and accounted for in accordance with the current HMG policy using a NCSC approved product or method. Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as a Storage Area Network (SAN) or shared backup tapes, then the Contractor or sub-contractor shall protect the Department's information and data until the time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.



- 1.16 Access by Contractor or sub-contractor staff to Departmental Data shall be confined to those individuals who have a “need-to-know” in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Department. All Contractor or sub-contractor staff must complete this process before access to Departmental Data is permitted.
- 1.17 The Contractor shall, as a minimum, have in place robust Business Continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the services delivered. If a ISO 22301 certificate is not available the supplier will provide evidence of the effectiveness of their ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures. This should include evidence that the Contractor has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.
- 1.18 Any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data being handled in the course of providing this service, or any non-compliance with these Departmental Security Standards for Contractors, or other Security Standards pertaining to the solution, shall be investigated immediately and escalated to the Department by a method agreed by both parties.
- 1.19 The Contractor shall ensure that any IT systems and hosting environments that are used to handle, store or process Departmental Data shall be subject to independent IT Health Checks (ITHC) using a NCSC approved ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Department and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.
- 1.20 The Contractor or sub-contractors providing the service will provide the Department with full details of any storage of Departmental Data outside of the UK or any future intention to host Departmental Data outside the UK or to perform any form of ICT management, support or development function from outside the UK. The Contractor or sub-contractor will not go ahead with any such proposal without the prior written agreement from the Department.
- 1.21 The Department reserves the right to audit the Contractor or sub-contractors providing the service within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being supplied and the Contractor’s, and any sub-contractors, compliance with the clauses contained in this Section.
- 1.22 The Contractor shall contractually enforce all these Departmental Security Standards for Contractors onto any third-party suppliers, sub-contractors or partners who could potentially access Departmental Data in the course of providing this service.



- 1.23 The Contractor and sub-contractors shall undergo appropriate security assurance activities as determined by the Department. Contractor and sub-contractors shall support the provision of appropriate evidence of assurance and the production of the necessary security documentation such as completing the DfE Security Assurance Model (DSAM) process or the Business Service Assurance Model (BSAM). This will include obtaining any necessary professional security resources required to support the Contractor's and sub-contractor's security assurance activities such as: a NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Professional (CCP) Security and Information Risk Advisor (SIRA)
- 1.24 Where the Contractor is delivering an ICT solution to the Department they shall design and deliver solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current NCSC Information Assurance Guidance and Departmental Policy. The Contractor will provide the Department with evidence of compliance for the solutions and services to be delivered. The Department's expectation is that the Contractor shall provide written evidence of:
- Existing security assurance for the services to be delivered, such as: PSN Compliance as a PSN Customer and/or as a PSN Service; NCSC (formerly CESG) Tailored Assurance (CTAS); inclusion in the Common Criteria (CC) or Commercial Product Assurance Schemes (CPA); ISO/IEC 27001 / 27002 or an equivalent industry level certification. Documented evidence of any existing security assurance or certification shall be required.
 - Existing HMG security accreditations or assurance that are still valid including: details of the body awarding the accreditation; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement. Documented evidence of any existing security accreditation shall be required.
 - Documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Contractor shall provide details of who the awarding body or organisation will be and date expected.

Schedule 3a

Processing, Personal Data and Data Subjects

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

1. The contact details of the Controller's Data Protection Officer are:
[REDACTED]
2. The contact details of the Processor's Data Protection Officer are:
[REDACTED]
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
4. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Department is the Controller and the Supplier is the Processor in accordance with Clause 17.1.
Subject matter of the processing	<p>The parties will Process Personal Data in the context of:</p> <ul style="list-style-type: none"> • Facilitating the supply of Databases, Discovery, eBooks, Periodicals and associated services as ordered by Department for Education using the supplier portals and other mechanisms • Routine customer service and account management in relation to this contract <p>This could include:</p> <ul style="list-style-type: none"> • Management of Department for Educations user accounts on the supplier portal • Distribution of information regarding development of the supplier's services • Distribution of information regarding availability of new materials or offers • Marketing information • Management information • Invoicing information



	<ul style="list-style-type: none">• EDI or API information transferred into Department for Education's library management system• E-mail communications regarding operational activity or queries in relation to the provision of services
Duration of the processing	The personal data will be processed for the length of the supplier relationship with Department for Education
Nature and purposes of the processing	<p>The Processing will be for the purposes of:</p> <ul style="list-style-type: none">• Facilitating the supply of Databases, Discovery, eBooks, Periodicals and associated services as ordered by Department for Education, and will require names, job titles, e-mail addresses and telephone numbers for Department for Education staff to be held on the supplier's ordering portal and in the customer relationship management tools.
Type of Personal Data	<p>The Personal Data will include:</p> <p>Names, job titles, telephone numbers and e-mail addresses of employees of Department for Education</p>
Categories of Data Subject	<p>The Data Subjects will include:</p> <p>Employees of Department for Education</p>
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	<p>The personal data will be processed for the length of the supplier relationship with Department for Education</p> <p>Upon termination of contract, or at any other time, Department for Education may request that EBSCO erase its data from its servers. Upon doing so, EBSCO will confirm that the information has been removed or destroyed. EBSCO maintains a Media Sanitation and Disposal policy regarding approved methods of destruction for various media types, including physical and electronic formats such as paper, optical disks (e.g., CD, DVD), magnet disks (e.g., floppy disks), magnetic tapes, hard drives, flash memory devices, portable devices (e.g. phones, tablets) and office equipment (e.g., network gear, fax machines, printers).</p>

Annex A – Statement of Requirements

DFE SPECIFICATION FOR ACADEMIC JOURNAL ACCESS

INTRODUCTION

The Department for Education (the Department or “DfE”) is seeking to establish a Contract for the electronic provision of Journal Subscriptions. This service should act as a ‘one stop shop’ arrangement for the Department’s journal access requirements that will provide access to required content. We would like a service that includes contingency arrangements in case the standard offer becomes temporarily inaccessible, for whatever reason, although our priority is alternative electronic access with print access as a last resort only. We also want to trial ebook access. The purpose of this specification is to provide a description of the Goods and Services that the Supplier shall be required to deliver to the Department.

BACKGROUND TO THE REQUIREMENT

The DfE is responsible for children’s services and education, including early years, schools, higher and further education policy, apprenticeships and wider skills in England. It has around 5,200 staff¹ and a budget of £64bn in 2019-20, although the bulk of this is then allocated by DfE to other bodies (e.g. £47.6bn for schools). The DfE spends around £29m a year on research and development². However we also need to learn from research from other organisations, both in the UK and internationally. Most high-quality scientific research funded outside government is published through academic journals. DfE needs access to as much relevant research evidence as possible to ensure that our advice to ministers and internal policy and delivery decisions are informed by the latest insight and evidence available. Advice is often needed quickly (sometimes within 24 hours), so we cannot wait for print copies or arranging access to specific articles. To help ensure our advice draws on the latest and most relevant research evidence we need readily available electronic access at our fingertips to as much *relevant* full text, UK and international English language publication as feasible.

DESCRIPTION OF THE REQUIREMENT - AIMS AND OBJECTIVES

The main aim of this procurement exercise is to replace the existing subscriptions held by the Department with a simpler, easy access solution offering broad and full text access to academic journals in DfE’s policy areas.

The desired outcome is a simpler system for electronic journals access, reducing the amount of time our users have to spend searching for relevant evidence, which also offers more comprehensive coverage than our current arrangements. We also want a service that will help us grow usage, be scalable and flexible as we develop a better understanding of

1. Source: <https://www.gov.uk/government/publications/dfe-monthly-workforce-management-information-2019-to-2020> Note: Workforce figures have not been published for several months owing to the General Election and the latest figures are likely to be higher.

² Source: <https://www.gov.uk/government/publications/dfe-consolidated-annual-report-and-accounts-2018-to-2019>

our users' needs and as those needs change. The system also has to meet Departmental security and confidentiality requirements.

Broad, full text coverage related to the Department's policy interests:

The focus of the content should first and foremost be on education, reflecting DfE's policy interests (from early years, through to primary, secondary, tertiary and higher education), but should encompass all of the Department's policy areas (including for example children's services) and disciplines in order to inform policy and delivery decisions. We have a particular interest in evidence from the UK but are also keen to learn from English-language literature from other countries. We also need as much full-text coverage as possible; users need to be able to access full-text to be able to provide appropriate briefing and advice. We also need to be able to access full-text quickly without having to request each individual article separately, through another system, and at additional expense and time. This also pertains to embargoes on most recent content; while we understand that publishers sometimes restrict the most recent content, we need a system that will provide the most up to date information possible in as seamless a way as possible.

We have not previously offered ebooks to our users but are keen to trial this in order to provide greater breadth of available information.

Simpler, easy access:

We want to make life as simple as possible for our users. In particular, at present our users have to search open access content, a number of databases, and individual journal subscriptions to find what they need. The more places that DfE staff have to search (including our own systems) and the more time it takes to find what they need, the less time they can spend on actively engaging with and using that evidence. There is also greater risk that they will not find the evidence they are looking for, not because it does not exist, but because searching proves too onerous and time consuming and the relevant source is missed. We want to reduce the amount of time our users have to spend searching for content by reducing the number of places our users have to search.

The successful supplier should provide an easy access, single portal that integrates ejournals (including open access content) and ebooks. The portal should allow simultaneous search of multiple journal sources, whether it is open access content, databases or (as far as possible) subscriptions to single journals held behind paywalls from different publishers.

We would also like the service to support users to obtain electronic full-text articles where these are not covered by our subscriptions. Currently users have to request this via email and arrangements are made via the British Library on demand or with the individual publisher. This would support our ambition of a more integrated service, but needs to have regard to copyright and to privacy and data protection requirements. We would especially welcome bids that can offer a service addressing those requirements. The Department is party to a Central Government copyright licence issued by the Copyright Licensing Agency which covers listed Central government organisations and staff to make and share copies from published works purchased or subscribed to by their organisation. The current licence runs until March 2021. The license permits the Department to receive unencrypted (DRM-free) copyright-fee paid documents from a range of suppliers including the British Library.



This enables the department to copy what we need when we need it without asking copyright owners' each time (within certain limits). Details can be found at <https://www.cla.co.uk/index.php/central-gov-licence>.

Ideally we want to incorporate Journals (and eBooks) access into our own (internally developed and hosted) Research Evidence Directory (RED). The aim of RED is to enable DfE staff to search research evidence held within DfE's systems and externally (including gov.uk research publications and our journals access) simultaneously. RED is intended to minimise the number of places that our users have to go to find relevant research evidence; essentially a "one stop shop". It is an internally developed and hosted web-based application. At minimum, the system (which is still in development – currently in "alpha") should be able to link via URL straight to the journals portal provided by the supplier with no need to log in or provide credentials. Where possible, suppliers should detail more advanced integrated approaches that could be provided. Suppliers should give details of the level of integration they can offer.

Helping us grow usage and flexibility to better meet changing user needs:

We also want to have a single journals (and ebooks) supplier who will manage our subscriptions and work with us to promote use and improve our coverage to better meet our users' needs throughout the duration of the contract. Currently we have to make renewal decisions for a number of subscriptions at various points during the year. We access monitoring information on usage to inform these decisions, extracting this from each source and then collating and analysing it ourselves. Ideally we would like a service that provides us with collated monitoring information for all of our subscriptions, and recommendations to help improve the service we can offer. This should be managed effectively as part of contract and performance management sessions (detailed further below).

The solution should be scalable, starting with access that suits the Department's needs with growth supported throughout the contract period, to reflect our plans to increase usage.

We require a supplier who can work flexibly with us and help us respond to changes in user needs, for example if machinery of government changes lead to changes in the Department's policy responsibilities.

Continuity of access and meeting needs for security and confidentiality:

We also need a solution that ensures continuity of access, which is consistent with the department's data security requirements, providing appropriate data protection and security (as detailed later in the specification).

DESCRIPTION OF SERVICES AND SCOPE

The Department requires the provision of a range of electronic academic and scientific journal collections covering the department's policy interests. This should act as a 'one stop shop' for the Department's journal access requirements.

The core content offering should be:

- Accessible to multiple users concurrently, but allowing for growth in usage.



- Academic scientific evidence only.
- Integrated electronic access to other, specific journals where needed and where not covered by the core offering.
- Integrated electronic open access content.
- Policy-relevant research content relevant to all DfE policy areas including early years, schools, further education, higher education and children's services.
- A high level of full-text access.
- UK and international English-language evidence.
- Management data on usage including search terms.
- It should be possible to click a link, and be taken straight to a specific search in the portal without having to log on

As above, while the content focus should be on all DfE policy areas including early years, schools, further education, higher education and children's services; we would welcome content from academic journals from related disciplines providing broader evidence, for example those that provide underpinning understanding on the impact of DfE policies, such as:

- Social science
- Sociology
- Psychology
- Economics
- Social Policy and Administration
- Political Science

We are also interested in:

- scientific evidence relevant to organisational and behaviour change which may (for example) be found in business journals
- scientific evidence relevant to children's services such as adoption which may be found in social work journals.
- research evidence on the latest and most effective research methods and analytical methods.

We are not looking for bids to provide news articles or law collections.

Our current collections are mainly provided through EBSCO and comprise of: Business Source Premier, Education Research Complete, Psychology and Behavioural Sciences, and SocINDEX with Full text. We also have subscribed to the OECD iLibrary and are interested in continuing this. Other relevant collections we could be interested in include (but are not limited to): ERIC (including as part of a wider collection giving additional full text access such as Education Collection), Education Source, EconLit, Sociology Source Ultimate, Social sciences full-text, Social Sciences database, Sociology database, and Social Science Premium Collection. We welcome bids that cover our subject interests.

We would be particularly interested in accessing the following journals through collections, which we had accessed through individual subscriptions in the past:

- British Journal of Educational Studies (Taylor & Francis)
- British Journal of Sociology of Education (Taylor & Francis)



- Educational Research (Taylor & Francis)
- Educational Review (Taylor & Francis)
- Educational Studies – UK (Taylor & Francis)
- Journal of Education Policy (Taylor & Francis)
- Oxford Review of Education (Taylor & Francis)
- Research Papers in Education (Taylor & Francis)
- School Leadership & Management (Taylor & Francis)
- Adoption and Fostering (Sage)
- Economics of Education Review (Elsevier)

Where these or other similar collections are included, the supplier should identify as part of their bid where these are standalone or where they are part of a wider database/collection. We would also welcome bids that include provision for academic e-books (text books) access on the core subject of education (focusing on academic literature), with scope to grow this to cover related subjects outlined above.

The supplier should be flexible in delivering the Department's requirements, in particular with relation to content (identifying heavily used content, unused material to be removed from scope and related content that would help improve coverage throughout the lifetime of the contract).

MANDATORY SERVICE REQUIREMENTS

Online Portal

The Supplier shall provide an 'online portal' enabling access to journal articles on a secure platform. The portal will need to offer comprehensive online search facilities. Ideally we would like a system that offers additional support where it is not possible to provide full-text. It should enable users to request that full text electronic access (or, where electronic access is not possible, for print copy). This could involve the request being sent to the DfE team overseeing the journals contract to decide case by case whether to pay for this access, or allow the system to authorise this up to an agreed budget ceiling. We would welcome advice on what could be offered to meet users' needs to access articles where they are not covered by our subscriptions, including on whether any individual articles could be added into the repository for wider use (should publishers allow this).

The Online Portal must provide access to electronic journals (whether through collections of journals or linking to individual titles), and shall include the following characteristics:

- An A-Z listing of all titles subscribed to (within each collection of the system is collection-based, or across other individual subscriptions).
- The ability to search by subject, author, journal and article title, and date of publication.
- The ability to search collections individually or all simultaneously.
- A clear indication of what is available, i.e. tables of content, abstract or full text.
- Concurrent user access is required (see Access section, below).
- The ability to restrict access according to licence conditions.



- The facility to set up alerts by title or subject (subject to ensuring appropriate use of personal data, privacy notices etc as referred to elsewhere herein).
- Easy to generate Management Information statistics on usage.
- Compliance with the requirements of the Equality Act 2010 regarding accessibility.
- Access to ebooks should be through the same portal if possible, or via a similar site.

Suppliers should explain what arrangements they can offer for connection to their portal(s) (e.g. authentication via IP address, Athens, Shibboleth, password logon or other means). This should take account of the Department's privacy and data protection requirements, and should not enable identification of individual staff in DfE.

Where possible the Supplier shall ensure that Electronic journals shall be available on the online portal rather than the Department having to separately access publisher's portals for view and download. Where this is not possible, the Supplier shall provide a link from their online portal to the publisher's portal for view and download of all journals subscribed to.

The Supplier shall ensure the online portal is compatible with browsers utilised by the Department (including current and previous versions of Microsoft Explorer, Edge, Google Chrome, Firefox and Safari).

The Supplier shall ensure its online portal remains compatible with any relevant future browser versions once they are released.

The Supplier shall ensure that the online portal is compatible and accessible with mobile devices, such as e-readers, tablets and Smart Phones.

Access

Secure Access to content shall be made available by the Supplier's portal or via a third party portal and shall be accessed by silent authentication or (if necessary) password activated (preferably using a department-wide login and password).

As a minimum, access should be available to 400 concurrent users in year 1, with the option to grow this to 700 users in year 2.

Access should not be through logins that identify individual users, but could be through logins that identify DfE users as a group, rather than individually, if necessary.

Renewals and Cancellations

We expect the Supplier will deal with renewals for any individual journals (whether as part of a collection or separate subscriptions) during the life of the contract. The Department expects to be able to change collection subscriptions during the life of the contract to better meet user needs, within the contract price. The Supplier should alert the Department to any individual journal subscriptions renewals at least three months prior to the subscription expiry date, or by an agreed date on an annual or twice-yearly basis.-

Renewal details provided to the Contracting Authority by the Supplier shall include title, price in pounds sterling, publisher and frequency of publication.

When the Department instructs a Supplier to cancel a subscription, the Supplier shall take action to ensure that the cancellation is effective immediately and that no further costs are incurred by the Contracting Authority. The Supplier shall accept Notice of cancellation via e-mail.

The Supplier shall advise the Department of any cancellation charges of either the publisher or the Supplier before cancellation is made and seek reconfirmation from the Contracting Authority that they still wish to cancel.

The Supplier shall acknowledge receipt of all cancellation requests within 5 (five) working days.

The Supplier shall ensure that where available a refund in respect of cancelled subscriptions is obtained from the publisher and credited to the Contracting Authority within seven (7) calendar days of receipt from the publisher.

Implementation, Training and Technical Support

The Supplier shall put in place an agreed implementation strategy, encompassing both contract mobilisation (see Contract Mobilisation further below), ongoing delivery and exit plans.

The Supplier shall be required to liaise with the Department's IT department in order to ensure accessibility through various intranet sites, portals and security systems to enable full fault free access.

The Department will provide a named contact in their IT department, who will provide the Supplier with all information necessary to deliver IT related Services.

The Supplier shall provide regular updates on progress and any issues, key risks identified during the implementation stage to the Department.

The Supplier shall provide training as agreed, free of charge to the Department in the use of its systems. This training may include but not limited to the following;

- user guides,
- online tutorials,
- webinars, and
- face-to-face sessions.

All online training formats shall be hosted by the Supplier's IT structure and should not require the Departments to download software onto their computers.

The Supplier shall be required to support their solution by means of a free customer and technical support help desk function for the Department. This shall be provided through webchat, email and telephone support.

The technical support help desk function shall be provided free of charge during office hours 9 am to 5 pm Monday to Friday as a minimum (excluding bank holidays).

The Supplier's help desk Personnel shall be fully trained and able to answer queries / questions quickly and efficiently. We expect it to be aligned to ITIL.

Sustainability and Social Value

The Supplier shall support the UK Government's commitment to ensure "green" economic growth by encouraging "green" technologies, promoting innovation, and protecting the environment whilst also delivering value for money.

The Supplier ensure they measure and reduce the sustainable impacts of their operations and supply-chains pertaining to the Goods and Services, and identifying opportunities to assist the Department in meeting their sustainability objectives.

Business Continuity and Disaster Recovery

The Supplier shall provide Business Continuity and Disaster Recovery plans to the Department upon signing the Contract. These should be reviewed by the Supplier annually or after any major incident and shared with the Department.

The Supplier shall have a robust Business Continuity Plan in place to maintain the delivery of Services during periods of unplanned unavailability the Online Portal and/or offline service(s).

The Supplier shall maintain its readiness with a Business Continuity plan in accordance with the principles and operation of ISO22301 and ISO22313 and any new or emergent or updated standards.

Confidentiality and Data Security

The Supplier will be required to comply with the Department's confidentiality and security standards as detailed in the draft contract (Annex C).

CONTRACT PERIOD

The contract will be for a 2 year period with an option to extend for a further year built into the contract.

CONTRACT MOBILISATION

Upon contract award, the successful supplier will work swiftly with the Department to outline a plan for mobilisation of the contract with a view to the solution being available for the Department to access by 15/04/2020. Activities including in this mobilisation plan should include but should not be limited to:

- Working with Department staff undertaking an IT Health Check, which the system has to pass before launch.
- Technical set up and integration with the Department's systems.
- Agreeing detailed plans for communications and publicity with users.
- Provision of training to end users and materials to support end users.

The plan should outline required actions, responsible owners for these actions and deadlines for achieving these actions. Any slippage against these milestones should be communicated to the Department as soon as possible.

PRICING, PAYMENT AND INVOICING

The Supplier shall comply with the Department requirements in respect of authorisation, invoicing and payment processes and procedures specified by individual Department which are set out in the draft contract (Annex C).

Invoices should be clearly addressed; and refer to the service provided and charging basis. The Supplier shall provide a full itemised breakdown of charges e.g. administration fees and any other additional charges indicated on the Supplier's invoice.

CONTRACT MANAGEMENT

The Supplier shall be required to appoint an account manager and a suitable deputy to cover periods of unavailability and absence, to attend all required meetings for the management of this Contract. The regularity of Contract Management meetings shall be agreed between the Department and the Supplier, but the Supplier should make provision for a minimum of one review meeting per quarter. Meetings will usually be held via Skype call unless otherwise agreed.

GENERAL PRINCIPLES

In delivering their services, the Department and the Supplier will adhere to the following operating principles, as set out below:-

User-centred

All parties will place a high priority on ensuring continuity and excellence of service to the users.

All parties will consider the needs of the user and/or named business area when making decisions. All parties will align performance of the service and associated measures with the needs of the DfE.

All parties will promote a "fix first; discuss later" principle, so that service to the business is prioritised.

Working cohesively

The Department and the Supplier will share opportunities and collaborate together to focus effort and drive continuous improvement. All parties will commit to work together to drive continuous service improvement.

The Supplier shall work with the Department with a view to reducing the costs and improving the quality and efficiency of the Goods and Services and their supply to the Department, an example of this may be additional discounts where multiple journal or ebook subscriptions are procured.

The Department shall expect the Supplier to support the government's targets to reduce spend by working with all Contracting Authorities to identify efficiencies in the buying of Goods and/or Services.

The Supplier shall identify new and potential improvements to the provision of the solution provided. This should include (but not be limited to) the use of management information to



identify additional collections that would enhance the offering, and may also include individual journal subscriptions not being used by the Department where this will offer best value in meeting the Department's needs. Flexibility should be applied by the supplier in managing this and enhancing the offering available to end users throughout the life of the contract.

Where it is identified that content is not being used by the Department, there should be the opportunity to cancel these subscriptions with a rebate provided or alternatively, replace this content with offerings that have been identified as potentially valuable to the Department.

Openness and honesty

All parties will seek to adopt a culture of openness and honesty to raise concerns and deal with difficult issues in a transparent, effective and timely manner.

Collaboration

All parties will co-operate, support and share information with each other, as is necessary, helping to deal with issues in the most effective way whilst removing barriers or delaying progress.

The Department will promote a collaborative culture where possible by including the Supplier in the making of decisions that affect them or at the least being open and transparent with a sensible lead time to impact assess and make changes.

Efficiency

All parties will work together to identify improvements, provide value for money and create a good working relationship to prevent recurring problems or issues.

All parties will aim to work in a planned manner giving each other as much notification of upcoming events or changes as is possible. The parties will at all times aim to comply with agreed lead times as per the contract.

At all times, where applicable the parties will ensure that the Department's policies and procedures are observed and followed and will comply with audit requests in this respect.



SERVICE LEVELS AND KEY PERFORMANCE INDICATORS

The following areas of focus will be measured within the contract in order to support effective delivery of the contract and drive good performance.

Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Threshold
Quality	User feedback	<p>Feedback from users to be recorded and used to create objectives for continuous improvement.</p> <p>This feedback can be collated by a reasonable agreed method between the supplier and the department.</p> <p>This will need to be collated before the quarterly review meetings for use.</p>	<p>Feedback to be reviewed biannually in supplier performance meetings.</p> <p>Minimum thresholds of user feedback ratings (to be agreed on a biannual basis) will be met at each quarterly point of measurement.</p>
Account Management	Availability and Timelines of MI and account management	<p>Provision of monthly MI and contract performance information to agreed format.</p> <p>Effective engagement to address queries to agreed timescales.</p> <p>Completion of all actions within an agreed timescale on a case by case basis.</p> <p>Attendance at quarterly performance meetings post quarterly MI.</p>	<p>Supplier response to queries within 3 working days. Actions completed within an agreed timescale on a case by case basis.</p> <p>Quarterly contract review meetings attended unless mutually rearranged within reasonable timeframes.</p>
Access to Customer Support	Availability and Service quality	<p>Customer service and support availability from 8am to 6pm Monday to Friday, excluding weekends and English bank holidays.</p> <p>Alternatively, if customer support is not immediately available a call back or email within 24 hours should be available to provide support.</p>	<p>Customer support should be available at least 98% of the time during core business hours (from 8am to 6pm Monday to Friday, excluding weekends and English bank holidays).</p>



Complaints and issues Handling	Acknowledgment and updates	<p>Complaints acknowledged within 24 hours and dealt with as a matter of priority.</p> <p>The supplier shall proactively work to seek a resolution and provide progress updates at intervals of 2 working days until a satisfactory resolution has been agreed mutually.</p>	95% of complaints successfully acknowledged and updated accordingly.
Training & support	Training to be provided and accessible.	<p>Online training and guidance should be available to users at all times.</p> <p>Customised training sessions for users should be provided within 1 month of the new solution's go live date.</p> <p>This training will support the end user's access to the journals and can be provided by multiple methods such as webinar and face to face.</p>	<p>Online training and guidance to be available at all times.</p> <p>All training sessions to be delivered in line with agreed training schedule.</p>
System	System issues/accesses (see also incident management below)	The system should be available for users to access 24/7, 365 days a year. Uptime should not fall below 99%. (with scheduled downtime, and successfully resolved incidents not being counted in these figures).	<p>Access to system available throughout core business hours.</p> <p>Planned system downtime should be communicated to users in advance of this taking place.</p>
Continuous improvement	Development of content availability	<p>Continuous improvement to work proactively and reactively to improve the departments journal access.</p> <p>Identifying areas for improvement in content accessed (identifying new</p>	<p>Requests for Change should be acknowledged within 2 working days and completed within 10 working days.</p> <p>Where the above is not possible, alternative timescales should be</p>



		valuable content and content that is not being used). Collaboration with the Department on integrating journals access into the Research Evidence Directory.	agreed with the Contract Manager in advance.
--	--	---	--

Incident Management

Incident Management on a per incident task basis will be the responsibility of the Supplier, The Supplier will aim to resolve all incident tasks within the targets set out below unless there is an acceptable reason for it to go on hold i.e. further information is required.

Service levels for incidents:

Priority	Target resolution within:	Definitions
1	4 working hours	<ul style="list-style-type: none"> • Application unavailable to all users • Majority of system application processes are failing • Failure of critical application function • Widespread corruption of critical data
2	8 working hours	<ul style="list-style-type: none"> • Application working at less than 50% efficiency • Less than 50% of application transactions are failing • Failure of important application function • Significant corruption of data
3	24 working hours	<ul style="list-style-type: none"> • Business process failed for non-critical deadline • Corruption of non-critical data
4	5 working days	<ul style="list-style-type: none"> • Non-Impacting Incident • Advice and Guidance

The Supplier will aim to resolve all incidents within the above targets unless there is an acceptable reason for it to have the due date revised i.e. further information is required.

For all Priority 1 incidents, identified during core service hours, 08.00-18.00, Monday to Friday, where applicable the managed supplier will manage and resolve these within the SLA of 4 hours.

The Supplier will investigate incidents and record their investigations. The Department will work with the Supplier to resolve incidents as needed.

The Department's contract manager will provide more information about user's feedback and will explain the appropriate incident severity scale to give based on the issue, urgency and impact. Urgency – how quick a resolution of the incident is required. Impact – extent of the issue and potential damage.

The DfE will expect the Supplier to report on following measures:

Service Measure	Target
-----------------	--------



% of Priority 1 Tasks resolved within 4 working hours	95%
% of Priority 2 Tasks resolved within 8 working hours	
% of Priority 3 Tasks resolved within 24 working hours	98%
% of Priority 4 Tasks resolved within 5 working days	
% of Category 1 Service Requests fulfilled within 5 working hours	95%
% of Category 2 Service Requests fulfilled within 2 working days	
% of Category 3 Service Requests fulfilled within 5 working days	
% of Category 1 Service Requests fulfilled within 22 working days	

Incidents that result from issues with the Department's systems will not be included in any such measures.

MANAGEMENT INFORMATION AND DATA REPORTING

The Supplier shall operate and maintain appropriate systems, processes and records to ensure that at all times it can deliver timely and accurate Management Information to the Department. Management Information will be provided to the Contract Management via email on a monthly basis in a consistent and agreed format. As well as monthly MI, a Quarterly highlight report should be provided to the Department in advance of each Contract Management meeting to support these sessions and continuous improvement throughout the life of the contract.

Areas of interest covered by Management Information should include (but not be limited to):

- Number of journals and collections accessed (split by collection).
- Highlight reporting on regularly accessed content and unused content.
- The number of times the system has been accessed.
- Details of additional requested content.
- The number of searches undertaken in the system (if possible, including whether any results were found and whether the content was accessed after searching).
- The number of full text journals that have been viewed compared with the number of abstracts viewed.
- The number of full text articles that have been downloaded.
- A record of the number of complaints and time taken for response and resolution.
- A record of the number of support issues and categorised reasons that the support was required (in accordance with the performance categories outlined above unless otherwise agreed).
- Details of any reported system issues or failures.

Management Information and data reporting shall be provided to the Contracting Authority free of charge.

TRANSITION AND EXIT

Upon request by the Department, the Supplier shall be required to produce an updated exit plan relating to the withdrawal from the Contract. This will be requested either before termination, or a minimum of three months prior to expiry of the contract. As a minimum the exit plan shall include:

- Management of resources;
- Lead times for phased withdrawal of Services;
- Timescales and indicative timeline;
- Communication plan to customers; and
- Handover of management information

The Supplier shall conduct a risk and issue analysis and identify and report to the Department all pertinent factors on a risk and issue log. All risks and issues identified shall be scored on a matrix such that likelihood of the risk or issue occurring is referenced against the impact severity should the risk or issue arise. All risks and issues shall consider staffing and employment issues and contingency/countermeasures. The risk and issue log shall identify all proposed mitigation to reduce or counter the risks and issues.

The exit plan will be treated as commercial in confidence, and is required to help both the Supplier and the Department deal with the risks and issues related to the expiry or termination of the Contract.

GDPR

The Supplier shall comply with the Department's Data Protection requirements as set out in the draft contract (Annex C). This will include the completion of Schedule 3 providing details of the Data Processor and Controller relationship and the data processed.

Annex B – Supplier Bid



Annex C – Pricing Schedule



Annex D – Licensing Agreement

Core contract terms will take precedence over terms outlined in this Annex.

