

**INVITATION TO TENDER LETTER**

Social Mobility Commission

Sanctuary Buildings,

Westminster, SW1P 3BT

Dear Researcher,

**INVITATION TO TENDER (ITT) for Apprenticeships and social mobility: fulfilling potential?**

1 Your organisation along with others is invited to offer a tender for provision of the above, to the specification outlined in the attached documents. Enclosed are:

[Document 1 Specification of the requirement.](#Document1)

[Document 2 Instructions on the tendering procedures.](#Document2)

[Document 3 Departmental standard requirements.](#Document3)

[Document 4 List of attachments.](#Document4)

[Document 5 Declaration and information to be provided by tenderer.](#Document5)

[Attachments Draft Terms and Conditions, Evaluation Criteria, Departmental Security Standards](#Attachment1)

2 Please read the instructions on the tendering procedures carefully. Failure to comply with them may invalidate your tender which must be returned by the date and time given below.

3 An electroniccopy of your tender must be submitted to [contact@socialmobilitycommission.gov.uk](mailto:contact@socialmobilitycommission.gov.uk) no later than **12 noon on 3rd May 2019**. Late tenders will **not** be considered.

4 If having read the enclosed specification you decide not to submit a tender, I would be grateful if could send your reasons (though you are under no obligation to do so) to [contact@socialmobilitycommission.gov.uk](mailto:contact@socialmobilitycommission.gov.uk), at the above address marked 'No Tender'.

5 Please contact me if you have any questions about the tendering procedure.

Yours sincerely,

Sasha Morgan,

Head of Secretariat, Social Mobility Commission

**DOCUMENT 1**

**SPECIFICATION**

**1 Introduction/Background**

The [Social Mobility Commission](https://www.gov.uk/government/organisations/social-mobility-commission) is inviting proposals for research to understand whether apprenticeships are serving to enhance individual apprentices’ social mobility opportunities.

Apprentices have great potential and promise to be a tool for social mobility. However, the reality may not be as clear cut. The Commission’s analysis in its State of the Nation 2018 points to unforeseen consequences on social mobility after recent policy and funding reforms. These include: reduced offerings at Levels 2 and 3, which offer a ‘foot on the ladder’ for disadvantaged students; reduced entry-level routes for young people into employment; reduced support for SMEs who provide entry-level routes, and; poor retention and progression for disadvantaged students.

The Commission is interested in apprenticeship selection, attrition, progression, quality of training, and outcomes by socioeconomic background. This research must include policy recommendations that could improve social mobility outcomes for apprentices.

**2 Purpose/Objectives**

The Commission is interested in the following research questions:

1. **What is the impact of recent apprenticeship policy reforms** (such as new standards and the levy) **on social mobility?**
2. **Selection**:
   1. What type of employers do disadvantaged apprentices work with through their apprenticeships compared to their non-disadvantaged peers?
   2. How does this change, if at all, when controlled for level of apprenticeship?
   3. Did the implementation of the levy change the type of employer disadvantaged apprentices work with?
   4. Geographically, where do disadvantaged apprentices take up apprenticeships?
3. **Training quality:**
   1. Do disadvantaged apprentices tend to work with firms who previously gave training prior to the levy?
   2. If not, are there differences in the quality of training or support that disadvantaged apprentices receive, as measured through relevant proxies?
4. **Attrition:**
   1. Does attrition from apprenticeships vary by socioeconomic background?
   2. Does this change, when controlling for or comparing by level of apprenticeship, and by age?
5. **Progression**:
   1. Where does progression happen within apprenticeships? For whom does it happen, by socioeconomic background?
   2. Are there differential outcomes associated with progression in the labour market by social background after completing an apprenticeship? Does this change for older compared to younger apprentices?
6. **Outcomes**:
   1. What are the labour market outcomes for disadvantaged apprentices, by level of apprenticeship taken, by socioeconomic background, and by course both before and after policy reforms?
   2. Do apprentices who repeat qualification levels gain a labour market return by doing so (i.e. those who already have a Level 3 qualification and then do a Level 3 apprenticeship)?

**Please note that we do not expect the researchers to answer every question in equal depth.** We also acknowledge that some questions may not be possible to answer, dependent on data limitations. We request that bidders indicate which questions and issues they will focus on primarily (using our suggestions from the ‘research considerations’ section below).

We envisage that this project will be quantitative, using administrative datasets such as LEO or the NPD linked to the ILR. Access to administrative datasets is crucial for this project, in order to assess social mobility outcomes.

This research is intended to allow the Commission to publish several short reports on the topic, in addition to the full final report. For example, short briefings on a) apprentices’ labour market outcomes b) comparisons between younger and older apprentices and c) progression routes for older and younger apprentices.

Research considerations and detail

* Age range: All those 16 and older. Researchers must follow the Government’s classification groupings for apprentices (i.e. 16-18, 19-24, and 25+).
* Prior studies: this work must build upon a growing body of research analysing the labour market returns to apprenticeships. This includes work by the Department for Education and the Centre for Vocational Education Research, as well as work done by the Commission.
* Data analysis: This will form the bulk of the research. This will build upon the descriptive data and analysis that the Commission has done in its State of the Nation 2018 report. More sophisticated analyses (e.g. regressions or Differences in Differences) will be needed and are at the discretion of the researcher to identify in bids.
* Outcomes: We are ultimately interested in social mobility (i.e. the link between an individual’s eventual occupation or earnings and the occupation or earnings of their parents).
* Regions: Where possible, please cut the data by broad region and area deprivation.
* Controls: Appropriate controls will need to be in place to allow conclusions to be drawn about the impact of apprenticeships on individuals’ attainment and employment outcomes.
* Measures of socioeconomic background: These could include any of, or a combination of, the common measures used by government. These include: eligibility for Free School Meals, parental education, parental occupation (measured by the NS-SEC), Indices of Multiple Deprivation, parental income, type of school attended, name of school attended, home postcode.
* Recommended data sources:
* NPD linked to ILR
* LEO
* Other datasets that researchers feel could appropriately answer the questions posed in sufficient depth.
* Bidders are permitted to sub-contract, but should indicate this clearly, with rationales, in the bids.

**3 Methodology**

Bidders are asked to set out the proposed methodology for answering the research questions. We do not expect every bid to answer each research question in a similar depth of detail.

While we do not restrict the quantitative methodology choices in this bid, we expect bidders to be clear on their selected methodological approaches. Sufficient methodological detail should be included in bids in order to show how research questions will be answered.

The Commission seeks ambitious and robust proposals. Bids will be judged on the proposed approach, expertise of team, and value for money.

Report drafting

The audience for this research will be UK policy makers, apprenticeship providers, employers, and stakeholders addressing social mobility issues, and the general public.

In addition to the final report, we would ideally publish a few short briefings on specific issues – including a separate report on any primary research conducted and/or a briefing on key findings – as well as the full final report. We hope this will generate media coverage of key issues and increase the public’s understanding of social mobility.

The final report should include full details of the methodology, data and analysis, and recommendations for policy changes. It is essential that proposed solutions to address any socio-economic gaps are included in the report.

All reports will be published on the Social Mobility Commission gov.uk website. This research will support the work of the Social Mobility Commission in developing our analysis and policy recommendations.

**4 Management Information**

The successful tenderer will be asked to provide management information to meet the needs of the Commission. The minimum information needs are:

* Three in-person meetings:
  + Kick-off meeting at the start of the project (no documentation required)
  + Mid-point review (requires a mid-point report) October 2019 to potentially feed into the Commission’s annual State of the Nation report
  + Final report (requires final reports) by the second week of March 2020
* Informal check-in meetings by phone or Skype every other month, in between the in-person meetings.
* A meeting(s), either in person or via phone or Skype to agree the structure and content of reports prior to their being drafted.
* Communication as needed, when barriers and challenges arise.

**5 Security of Data**

Please submit a security plan that explains how you will ensure that departmental or personal data will be protected.

**6 Risk Management**

Tenderers should submit as part of their proposal a one-page summary on what they believe will be the key risks to delivering the project and what contingencies they will put in place to deal with them.

A risk is any factor that may delay, disrupt or prevent the full achievement of a project objective. All risks should be identified. For each risk, the one-page summary should assess its likelihood (high, medium or low) and specify its possible impact on the project objectives (again rated high, medium or low). The assessment should also identify appropriate actions that would reduce or eliminate each risk or its impact.

Typical areas of risk for a research project might include staffing, resource constraints, technical constraints, data access, timing, management and operational issues, but this is not an exhaustive list.

**6 Dependencies and Liason**

Tenderers should indicate if they are reliant on any third party with any information, data or undertaking any of the work specified.

**7 Monitoring Techniques**

Tenderers should indicate how you will monitor the project to ensure it is delivered in terms of quality, timeliness and cost.

**8 Data Collection**

Researchers will be expected to clear any data collection tools with the Commission before engaging in field work and ensure that in all cases the respondent documentation and/or interviewer briefing notes clearly state that the data is being collected for and on behalf of the Commission and that no reference is made, implied or otherwise, to the data being used solely by or available only to the Contractor.

The respondent documentation and/or interviewer shall ensure that the respondent clearly understands (before they give their consent to be interviewed) the purpose of the interview, that the information they provide will only be used for research purposes and, in the case of interviews (telephone or face-to-face), that they have the right to withdraw from the interview at any time.

SMC seeks to minimise the burdens on schools and Local Authorities (LAs) taking part in surveys. It is therefore important that tenders should set out how the proposed methodology will minimise the burden on schools and/or LAs and a justification for the proposed sample size.

When assessing the relative merits of data collection methods the following issues should be considered:

* only data essential to the project shall be collected;
* data should be collected electronically where appropriate and where schools and/or LAs prefer this;
* questionnaires should be pre-populated wherever possible and appropriate;
* schools must be given at least four working weeks to respond to the exercise from the date they receive the request; and
* LAs should receive at least two weeks, unless they need to approach schools in which case they too should receive 4 weeks to respond.

The Contractor shall clear any data collection tools with the Commission before engaging in field work.

Researchers shall check with the Commission whether any of the information that they are requesting from schools can be provided centrally from information already held.

**9 Consent Arrangements**

The Commission and the successful contractor shall agree in advance of any survey activity taking place the consent arrangements that shall apply for each of the participant groups. All participants should be informed of the purpose of the research, that the Contractor is acting on behalf of the Commission and that they have the option to refuse to participate (opt out). Contact details should be provided including a contact person at the Commission. Children who are 16 or over will usually be able to give their own consent but even where this is so, the Contractor, in consultation with the Commission, should consider whether it is also appropriate for parents, guardians or other appropriate gatekeepers (e.g. schools, Local Authorities) to be informed when a child has been invited to participate in research.

**10 Costs and Budget**

We estimate the research should cost between £80,000-£100,000 in total (excluding VAT). Please note that budget flexibility is provided for those wishing to include qualitative elements. Strong rationale for such qualitative pieces is necessary to determine sufficient value for money.

All costs should be quoted exclusive of VAT but please indicate if the project will attract VAT.

If your proposal includes costs for sub-contractors these costs must be shown inclusive of any VAT element (e.g. sub-contractor’s costs to you are £5,000 plus VAT, your proposal should show sub-contractors costs as £6,000 inclusive of VAT @ 20%).

**10.1** A detailed breakdown of costs is required within the proposal (excluding VAT).

Your tender should provide a detailed breakdown of costs on the basis of:

* project management and professional time;
* survey costs (if applicable);
* secretarial and administrative costs;
* travel and subsistence (please note details below);
* stationery, postage and telephone; and

publicity.

Costs should be shown separately by financial year and where more than one type of methodology is involved the costs need to be shown separately for each element, e.g:

* group discussions;
* personal interview;
* telephone survey;
* postal survey; and
* desk research.

**10.2** Payments will be made by BACS transfer following receipt of a valid invoice.

**10.3** The successful tenderer should provide details of discounts for prompt payment.

**11 Incentives**

With some important exceptions, SMC believes that the routine use of respondent incentives in surveys is, in general, not justified as they are rarely cost effective in either increasing participation or reducing non-response biases. If you are proposing the use of respondent incentives in your tender proposal you must set out why you feel they are necessary, why it is not possible to achieve the required sample sizes or response rates without the use of incentives, how and to what extent they will raise the overall response rate, how you will mitigate any specific biases that could be introduced, and provide a cost comparison with non-incentive methods. Your arguments should be supported by empirical evidence from past use. The exceptions are payment for participation in group discussions or in-depth qualitative interviews, payment to cover respondent expenses e.g. travel and childcare costs, and compensation for excessive demand on respondents, e.g. taking basic skills tests, diary keeping, panel maintenance and compensating schools for the respondent’s time. If you wish to use a prize draw incentive then you must also set out in your tender how you will comply with all relevant legislation and codes of practice (e.g. the British Code of Advertising and Sales Promotion), state that you shall be solely liable for any breach of these and that you shall indemnify SMC against any claims that may be made under them.

**12 VAT**

12.1Please state clearly when submitting prices whether or not VAT will be charged.

12.2 Where the contract price agreed between SMC and contractor is inclusive of any VAT, further amounts will not be paid by SMC should a vatable supply claim be made at any later stage.

12.3 Where the overall contract price is exclusive of VAT, SMC will pay any VAT incurred at the prevailing rate (currently 20%). If the VAT rate changes SMC will pay any VAT incurred at the new rate.

12.4 It is the responsibility of tenderers to check the VAT position with HMRC before submitting a bid.

**13** Not Used

**14** Not Used

**DOCUMENT 2**

**INSTRUCTIONS ON TENDERING PROCEDURES**

1 These instructions are designed to ensure that all tenders are given equal and fair consideration. It is important therefore that you provide all the information asked for in the format and order specified. Please contact **contact@socialmobilitycommission.gov.uk** if you have any doubts as to what is required or you have difficulty in providing the information requested. Pre-tender negotiations are notallowed.

2 Please note that references to the 'Department' or “Social Mobility Commission” or “the Commission” throughout these documents mean The Secretary of State for Education acting through his representatives in the Department for Education.

3 SMC is happy to accept bids from single organisations or consortia of organisations. Where a consortium/Special Purpose Vehicle (SPV) is formed to submit a tender, this must only be submitted by and in the name of, the supplier chosen as the “Lead” supplier for that consortium/SPV.

**Contract Period**

3 The contract is to be completed by March 2020, with the potential to renew for 6 months if negotiated and agreed between SMC, the supplier, and the Department.

**Incomplete Tender**

4 These instructions are designed to ensure that all tenders are given equal and fair consideration. Tenders may be rejected if the information asked for in the ITT and Specification is not given at the time of tendering.

**Indicative procurement timetable**

5 The indicative timetable for the procurement is:

|  |  |
| --- | --- |
| Tender documents issued | 5th April 2019 |
| Last day for submission of clarifications | 24th April |
| Last day for SMC to respond to clarifications | 26th April |
| Deadline for tender responses to be received | 3rd May |
| Tender Evaluations | 3rd May – 20th May |
| Department announcement of preferred bidder | By w/c 20th May |
| Contract fine-tuning with preferred bidder to take account of the solution | By w/c 27th May |
| Contract commencement | 3rd June |

**Returning Tenders**

6 Please send your proposal by email to: [**contact@socialmobilitycommission.gov.uk**](mailto:contact@socialmobilitycommission.gov.uk) Subject line of the email should read ‘Research Bid’. Tenders must be delivered by **3rd May at 12 noon.** Confirmations that bids have been received will be sent after the closing day. SMC will publish clarifications on Contracts Finder by 26 April.

**Receipt of Tenders**

7 Tenders will be received up to the time and date stated. Those received before the due date will be retained unopened until then. It is the responsibility of the tenderer to ensure that their tender is delivered not later than the appointed time.

**Acceptance of Tenders**

8 By issuing this invitation SMC is not bound in any way and does not have to accept the lowest or any tender, and reserves the right to accept a portion of any tender, unless the tenderer expressly stipulates otherwise in their tender.

9 SMC reserves the right to treat any tender which is caveated by reference to the UK exiting the EU with a deal or without a deal as non-compliant and, as with any procurement exercise, a bidder in submitting its price for evaluation does so in acceptance of all business risks and circumstances arising from time to time.

**Inducements**

10 Offering an inducement of any kind in relation to obtaining this or any other contract with SMC will disqualify your tender from being considered and may constitute a criminal offence.

**Confidentiality of Tenders**

11 Please note the following requirements, you must not:

1. Tell anyone else what your tender price is or will be, before the time limit for delivery of tenders.
2. Try to obtain any information about anyone else's tender or proposed tender before the time limit for delivery of tenders.
3. Make any arrangements with another organisation about whether or not they should tender, or about their or your tender price.

Failure to comply with these conditions may disqualify your tender.

**Costs and Expenses**

12 You will not be entitled to claim from SMC any costs or expenses which you may incur in preparing your tender whether or not your tender is successful.

**Debriefing**

13 Following the award of contract, debriefing will be available to unsuccessful tenderers on request.

**Evaluation Criteria**

14 The tender process will be conducted in a manner that ensures tenders are evaluated fairly to ascertain the economically most advantageous tender.

15 Not Used

16 Your response to the tender specification will be evaluated using the criteria set out in Document 4 Section 2 - Evaluation Criteria.

**Tender Period**

17 Due to the intensive evaluation process SMC requires tenders to remain valid for a period specified in Document 5.

**Basis of the Contract**

18 The specification in Document 1, and the terms and conditions in Document 4 Attachment 1, together with any special requirements, will form the basis of the contract between the successful tenderer and the Secretary of State for Education.

**Format of Bids**

19 Tenderers should present their proposals in the following format:

**Section 1 Summary of Proposal**

**Section 2 Meeting the Specification:**

1. Details of proposed approach;
2. Methodology, including constraints and possible solutions;
3. Project management;
4. Staffing, including examples of key relevant experience and individual/staff expertise and qualifications. Proposed distribution of duties should be clearly stated if the bid involves sub-contracting or collaboration between different providers; and
5. Outputs, including how the findings will be presented.

**Section 3 Cost and Charging Arrangements**

* Costs should be shown separately by financial year and where more than one type of methodology is involved the costs need to be shown separately for each element, e.g.:

1. group discussions;
2. personal interview;
3. telephone survey;
4. postal survey; and
5. desk research.

**Section 4 Risk Management**

**Section 5 Data Security**

**Section 6 References**

**Section 7 Declarations, Undertakings and Attachments** (see Document 5)

Sections 1 - 4 should not exceed 7 sides of A4 and sections 5 - 6 should not exceed 3 sides of A4, for a combined **total of 10 pages**. Any bids above that will be not be considered.

**Conclusions**

20 Whilst every endeavour has been made to give tenderers an accurate description of the Commission’s requirement, tenderers should make their own assessment about the methods and resources needed to meet those requirements.

**DOCUMENT 3**

**DEPARTMENTAL STANDARD REQUIREMENTS**

**Freedom Of Information**

1 SMC is committed to open government and to meeting their responsibilities under the Freedom of Information Act 2000. Accordingly, all information submitted to SMC may need to be disclosed in response to a request under the Act. If you consider that any of the information included in your tender is commercially sensitive, please identify it and explain (in broad terms) what harm may result from disclosure if a request is received, and the time period applicable to that sensitivity. You should be aware that, even where you have indicated that information is commercially sensitive, we may still be required to disclose it under the Act if a request is received. Please also note that the receipt of any material marked ‘confidential’ or equivalent by SMC should not be taken to mean that we accept any duty of confidence by virtue of that marking. If a request is received, we may also be required to disclose details of unsuccessful tenders.

**Publication of Contract**

2 Under the Government’s Transparency requirements we are obliged to publish the contract between SMC and the successful tenderer(s) in full. The successful tenderer(s) should identify any information regarded as commercially sensitive and explain (in broad terms) what harm may result from disclosure and the time period applicable to that sensitivity. You should be aware that, even where you have indicated that information is commercially sensitive, we may still be required to disclose it if the public interest in disclosure outweighs withholding the information. See ‘[The Transparency of Suppliers and Government to the Public](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/592358/TransparencyPrinciplesFebruary2017.pdf)’ for more detail.

**Information Sharing Across Government**

3 All Central Government Departments and their Executive Agencies and Non Departmental Public Bodies are subject to control and reporting within Government. In particular, they report to the Cabinet Office and HM Treasury for all expenditure. Further, the Cabinet Office has a cross-Government role delivering overall Government policy on public procurement - including ensuring value for money and related aspects of good procurement practice.

4 For these purposes, SMC may disclose within Government any of the Contractor's documentation/information (including any that the Contractor considers to be confidential and/or commercially sensitive such as specific bid information) submitted by the Contractor to SMC during this Procurement. The information will not be disclosed outside Government. Contractors taking part in this competition consent to these terms as part of the competition process.”

**Cyber Essentials Scheme**

5 The Government has introduced its new Cyber Essentials Scheme in consultation with industry to mitigate the risk from common internet based threats.

6 It is mandatory for new Central Government contracts, which feature characteristics involving the handling of personal data and ICT systems designed to store or process data at the OFFICIAL level of the [Government Security Classifications scheme](https://www.gov.uk/government/publications/government-security-classifications) to comply with Cyber Essentials requirements.

7 All potential tenderers for Central Government contracts, featuring the above characteristics, should make themselves aware of [Cyber Essentials](https://www.gov.uk/government/publications/cyber-essentials-scheme-overview) and the requirements for the appropriate level of certification “or equivalent”.

8 As this requirement features the above characteristics, you are required to demonstrate in your tender response that:

* Your organisation will be able to secure **Cyber Essentials** certification prior to contract award; or
* Your organisation has equivalent evidence to support that you have appropriate technical and organisational measures to mitigate the risk from common internet based threats in respect to the following five technical areas:

1. Boundary firewalls and internet gateways - these are devices designed to prevent unauthorised access to or from private networks, but good setup of these devices either in hardware or software form is important for them to be fully effective.
2. Secure configuration – ensuring that systems are configured in the most secure way for the needs of the organisation
3. Access control – Ensuring only those who should have access to systems to have access and at the appropriate level.
4. Malware protection – ensuring that virus and malware protection is installed and is up to date
5. Patch management – ensuring the latest supported version of applications is used and all the necessary patches supplied by the vendor have been applied.

Any equivalent evidence must be verified by a technically competent and independent third party.

9 The successful tenderer will be required to provide evidence of **Cyber Essentials** certification “or equivalent” (i.e. demonstrate they meet the five technical areas the Cyber Essentials Scheme covers) prior to contract award.

10 The successful tenderer will be required to secure and provide evidence of **Cyber Essentials** re-certification “or equivalent” (i.e. demonstrate they meet the five technical areas) on an annual basis.

11 Details of certification bodies are available at: <https://www.cyberstreetwise.com/cyberessentials>

**Data Security Standards**

12 For contracts which require the holding or processing of either personal data and/or OFFICIAL data the successful contractor will need to assure SMC that they can comply with the Department’s security standards.

13 Departmental security standards are listed as contract clauses in an annex to this letter (see Document 4 – List of Attachments).

**Prompt Payment Policy**

14 Government’s aim is to pay 80% of all correctly submitted invoices within 5 days of receipt and we are 100% committed to paying correctly submitted invoices within 30 days of receipt from the day of physical or electronic arrival at the nominated address of the Department.

15 The payment period will be deemed to have started when a correctly submitted invoice reaches the nominated address or emailed to contact@socialmobilitycommission.gov.uk. Contractors can assume receipt to be two days after mailing (by first class post). The thirty day “clock” therefore commences two days after mailing first class.

16 A correct invoice is one that is:

* delivered in timing in accordance with the contract;
* that 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);
* include the date, supplier name, contact details and bank details;
* which quote the relevant purchase order / contract reference;
* which has been delivered to the nominated address.

17 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.

**Sub-contracting to Small and Medium Enterprises (SMEs)**

18 SMC is committed to removing barriers to SME participation in its contracts, and would like to also actively encourage its larger suppliers to make their sub-contacts accessible to smaller companies and implement SME-friendly policies in their supply-chains.  This can be achieved by advertising subcontracting opportunities on Contracts Finder and implementing the principles of the SME and Growth Agenda in your own organisation.

19 To help us measure the volume of business we do with SMEs, we will be asking SMC suppliers to provide us with information about the size of your own organisation and those in your supply chain.   We may ask about volumes of business that will flow from this contract down your supply chains, and ask you to quantify that for us.   This data will help us contribute towards Government targets on the use of SMEs. We may also publish success stories and examples of good practice on our website.

20 Not Used

**Armed Forces Covenant**

21 The Armed Forces Covenant is a public sector pledge from Government, businesses, charities and organisations to demonstrate their support for the armed forces community. The Covenant was brought in under the Armed Forces Act 2011 to recognise that the whole nation has a moral obligation to redress the disadvantages the armed forces community face in comparison to other citizens, and recognise sacrifices made.

22 The Covenant’s 2 principles are that:

• the armed forces community should not face disadvantages when compared to other citizens in the provision of public and commercial services.

• special consideration is appropriate in some cases, especially for those who have given most such as the injured and the bereaved.

23 The Department encourages all Tenderers, and their suppliers, to sign the Corporate Covenant, declaring their support for the Armed Forces community by displaying the values and behaviours set out therein.

24 Guidance on the various ways you can demonstrate your support through the Corporate Covenant is at [The Corporate Covenant](https://www.gov.uk/government/policies/armed-forces-covenant).

25 If you wish to register your support you can provide a point of contact for your company on this issue to the Armed Forces Covenant Team at the address below, so that the MOD can alert you to any events or initiatives in which you may wish to participate. The Covenant Team can also provide any information you require in addition to that included on the website.

Email address: covenant-mailbox@mod.uk

Address: Armed Forces Covenant Team

Zone D, 6th Floor, Ministry of Defence,

Main Building, Whitehall, London, SW1A 2HB

26 Paragraphs 20-25 above are not a condition of working with SMC now or in the future, nor will this issue form any part of the tender evaluation, contract award procedure or any resulting contract. However, SMC very much hopes you will want to provide your support.

**Conflicts of interest**

27 SMC may exclude an organisation if there is a conflict of interest which cannot be effectively remedied. The concept of a conflict of interest includes any situation where relevant staff members have, directly or indirectly, a financial, economic or other personal interest which might be perceived to compromise their impartiality and independence in the context of the procurement procedure.

28 Where there is any indication that a conflict of interest exists or may arise then it is the responsibility of the organisation to inform SMC, detailing the conflict in a separate Appendix. Provided that it has been carried out in a transparent manner, routine pre-market engagement carried out by SMC should not represent a conflict of interest for the organisation.

**Disability Confident Scheme**

29 The Department for Education is a Disability Confident leader. Through the Disability Confident campaign, the government is working with employers to remove barriers, increase understanding and ensure that disabled people have the opportunities to fulfil their potential and realise their aspirations.

30 SMC encourage other employers to sign up to the disability confident scheme. It is open to all employers and there are three levels ranging from ‘Committed’ to ‘Leader’ with employers having to meet certain criteria to reach each level.

31 Employers who sign up to the disability confident scheme ensure that they can:

* draw from the widest possible pool of talent;
* secure and retain high quality staff who are skilled, loyal and hard working;
* save time and money on the costs of recruitment and training by reducing staff turnover;
* keep valuable skills and experience;
* reduce the levels and costs of sickness absences; improve employee morale and commitment by demonstrating that they treat all employees fairly.

32 Disability confident employers can use the disability confident branding in their communications and when advertising jobs.

33 Find out more about the aims of disability confident, why becoming a disability confident employer will be good for your business and how you will be supported through your journey to being a Disability Confident leader [here](https://www.gov.uk/guidance/disability-confident-how-to-sign-up-to-the-employer-scheme).

**Safe Guarding Children and Vulnerable Adults**

34 The standard Terms and Conditions include provisions to put in place safeguards to protect children and vulnerable adults from a risk of significant harm which could arise from the performance of this Contract. The potential Contractor will agree these safeguards with SMC before commencing work on the Contract.

35 In addition, the potential Contractor will carry out checks with the Disclosure and Barring Service (DBS checks) on all staff employed on the Contract in a Regulated Activity. The DBS check must be completed before any of the Contractor’s employees work with children in Regulated Activity.

**DOCUMENT 4**

**LIST OF ATTACHMENTS**

1. **DRAFT TERMS AND CONDITIONS**

**2 EVALUATION CRITERIA**

Scoring scale

|  |  |
| --- | --- |
| *0* | Nil or inadequate response. Fails to demonstrate an ability to meet the requirement. |
| *1* | Response meets less than half the stated requirement. It is partially relevant but generally poor and lacks relevant detail. |
| *2* | Response meets some but not all of the stated requirement. Lacks detail on how the requirement will be fulfilled in several areas. |
| *3* | The response meets the stated requirement. Answers are relevant and acceptable but may lack some detail. |
| *4* | The response fully meets the stated requirement in all areas. Answers are clear, relevant and elements of the response exceed the requirement by offering some added value. |
| *5* | The response exceeds the requirement in all areas. Answers are comprehensive, unambiguous and offer significant added value to the requirement which benefits SMC. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ref | Question | Look for’s | Weight | Maximum possible score |
| 1 | Does the proposal describe a robust method / suitable approach? | * Demonstrates a clear understanding of the policy area, the requirements of this type of study, and role it provides * Constructive thinking demonstrated by the proposed methodological approach to this project in meeting the objectives (including identifying and addressing risks) * The suitability of the proposed approach to deliver against requirements of the study, and identification of any opportunities to add value to this * Consideration of ethical, confidentiality and data protection issues * That the risks and challenges are considered and mitigation integrated into the proposed methodology * The quality, timing and suitability of proposed outputs, and potential to inform and influence both policy and delivery | **6** | **30** |
| 2 | Team and organisational experience in conducting research | * Experience of staff in relevant research techniques * Experience of specific research in this area and familiarity with subject area * Evidence of experience in the challenges and considerations involved in the relevant type of research * How the skills and experience of the team will be used and managed to best effect (where there is a partnership please include specific about how this will be managed, add value and any experience of successful collaboration) * Clear plan for communication and demonstration of a collaborative approach to taking the work forward, working closely with SMC as appropriate * Evidence of organisational capacity, project management and risk-management processes, and quality assurance procedures, to deliver the project in the specified timescales and quality | **6** | **30** |
| 3 | Presentation of data, findings and recommendations | * Clear articulation of plans for presenting the findings in clear and eye-catching ways * Evidence of ability to deliver high quality research, fieldwork and outputs * Ability to write good quality reports with clear findings and workable recommendations, tailored to their audiences | **4** | **20** |
| 4 | Cost and value for money | * Overall scope, quality and timeliness of the project for the given costs * Proposed costs are expected to be commensurate with the potential to deliver quality, capacity and timeliness, and meets and / or exceeds the requirements (provides added value), and value for money will be assessed as such | **4** | **20** |

Scoring Example

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Supplier A Score** | **Supplier B Score** | **Supplier Score** |
| Proposal | 3 (score) x (weight) 6 = 18 | 4 (score) x (Weight) 6 = 24 | 5 (score) x (weight) 6 = 30 |
| Experience | 3 (score) x (weight) 6 = 18 | 4 (score) x (Weight) 6 = 24 | 3 (score) x (weight) 6 = 18 |
| Presentation | 4 (score) x (weight) 4 = 16 | 4 (score) x (Weight) 4 = 16 | 4 (score) x (weight) 4 = 16 |
| Value for Money | 2 (score) x (weight) 4 = 8 | 4 (score) x (Weight) 4 = 16 | 3 (score) x (weight) 4 = 12 |
| **Total** | 60 | **80 (Highest Score)** | 76 |

**DOCUMENT 5**

**DECLARATIONS AND INFORMATION TO BE PROVIDED BY THE TENDERER**

**1 Grounds for mandatory exclusion**

You will be excluded from the procurement process if there is evidence of convictions relating to specific criminal offences including, but not limited to, bribery, corruption, conspiracy, terrorism, fraud and money laundering, or if you have been the subject of a binding legal decision which found a breach of legal obligations to pay tax or social security obligations (except where this is disproportionate e.g. only minor amounts involved).

Please answer the following questions in full. Note that every organisation that is being relied on to meet the selection must complete and submit the self-declaration.

|  |  |  |
| --- | --- | --- |
| 2 | Grounds for mandatory exclusion | |
| Question number | Question | Response |
| 2.1(a) | **Regulations 57(1) and (2)**  The detailed grounds for mandatory exclusion of an organisation are set out on this [web page](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551130/List_of_Mandatory_and_Discretionary_Exclusions.pdf), which should be referred to before completing these questions.  Please indicate if, within the past five years you, your organisation or any other person who has powers of representation, decision or control in the organisation been convicted anywhere in the world of any of the offences within the summary below and listed on the [webpage](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551130/List_of_Mandatory_and_Discretionary_Exclusions.pdf). | |
|  | Participation in a criminal organisation. | Yes ☐  No ☐  If Yes please provide details at 2.1(b) |
|  | Corruption. | Yes ☐  No ☐  If Yes please provide details at 2.1(b) |
|  | Fraud. | Yes ☐  No ☐  If Yes please provide details at 2.1(b) |
|  | Terrorist offences or offences linked to terrorist activities | Yes ☐  No ☐  If Yes please provide details at 2.1(b) |
|  | Money laundering or terrorist financing | Yes ☐  No ☐  If Yes please provide details at 2.1(b) |
|  | Child labour and other forms of trafficking in human beings | Yes ☐  No ☐  If Yes please provide details at 2.1(b) |
| 2.1(b) | If you have answered yes to question 2.1(a), please provide further details.  Date of conviction, specify which of the grounds listed the conviction was for, and the reasons for conviction,  Identity of who has been convicted  If the relevant documentation is available electronically please provide the web address, issuing authority, precise reference of the documents. |  |
| 2.2 | If you have answered Yes to any of the points above have measures been taken to demonstrate the reliability of the organisation despite the existence of a relevant ground for exclusion ? (Self Cleaning) | Yes ☐  No ☐ |
| 2.3(a) | **Regulation 57(3)**  Has it been established, for your organisation by a judicial or administrative decision having final and binding effect in accordance with the legal provisions of any part of the United Kingdom or the legal provisions of the country in which the organisation is established (if outside the UK), that the organisation is in breach of obligations related to the payment of tax or social security contributions? | Yes ☐  No ☐ |
| 2.3(b) | If you have answered yes to question 2.3(a), please provide further details. Please also confirm you have paid, or have entered into a binding arrangement with a view to paying, the outstanding sum including where applicable any accrued interest and/or fines. |  |

Please Note: SMC reserves the right to use its discretion to exclude a potential supplier where it can demonstrate by any appropriate means that the potential supplier is in breach of its obligations relating to the non-payment of taxes or social security contributions.

|  |  |  |
| --- | --- | --- |
| 3 | Grounds for discretionary exclusion | |
|  | Question | Response |
| 3.1 | **Regulation 57 (8)**  The detailed grounds for discretionary exclusion of an organisation are set out on this [web page](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551130/List_of_Mandatory_and_Discretionary_Exclusions.pdf), which should be referred to before completing these questions.  Please indicate if, within the past three years, anywhere in the world any of the following situations have applied to you, your organisation or any other person who has powers of representation, decision or control in the organisation. | |
| 3.1(a) | Breach of environmental obligations? | Yes ☐  No ☐  If yes please provide details at 3.2 |
| 3.1 (b) | Breach of social obligations? | Yes ☐  No ☐  If yes please provide details at 3.2 |
| 3.1 (c) | Breach of labour law obligations? | Yes ☐  No ☐  If yes please provide details at 3.2 |
| 3.1(d) | Bankrupt or is the subject of insolvency or winding-up proceedings, where the organisation’s assets are being administered by a liquidator or by the court, where it is in an arrangement with creditors, where its business activities are suspended or it is in any analogous situation arising from a similar procedure under the laws and regulations of any State? | Yes ☐  No ☐  If yes please provide details at 3.2 |
| 3.1(e) | Guilty of grave professional misconduct? | Yes ☐  No ☐  If yes please provide details at 3.2 |
| 3.1(f) | Entered into agreements with other economic operators aimed at distorting competition? | Yes ☐  No ☐  If yes please provide details at 3.2 |
| 3.1(g) | Aware of any conflict of interest within the meaning of regulation 24 due to the participation in the procurement procedure? | Yes ☐  No ☐  If yes please provide details at 3.2 |
| 3.1(h) | Been involved in the preparation of the procurement procedure? | Yes ☐  No ☐  If yes please provide details at 3.2 |
| 3.1(i) | Shown significant or persistent deficiencies in the performance of a substantive requirement under a prior public contract, a prior contract with a contracting entity, or a prior concession contract, which led to early termination of that prior contract, damages or other comparable sanctions? | Yes ☐  No ☐  If yes please provide details at 3.2 |
| 3.1(j)  3.1(j) - (i)  3.1(j) - (ii)  3.1(j) –(iii)  3.1(j)-(iv) | Please answer the following statements  The organisation is guilty of serious misrepresentation in supplying the information required for the verification of the absence of grounds for exclusion or the fulfilment of the selection criteria.  The organisation has withheld such information.  The organisation is not able to submit supporting documents required under regulation 59 of the Public Contracts Regulations 2015.  The organisation has influenced the decision-making process of the contracting authority to obtain confidential information that may confer upon the organisation undue advantages in the procurement procedure, or to negligently provided misleading information that may have a material influence on decisions concerning exclusion, selection or award. | Yes ☐  No ☐  If Yes please provide details at 3.2  Yes ☐  No ☐  If Yes please provide details at 3.2  Yes ☐  No ☐  If Yes please provide details at 3.2  Yes ☐  No ☐  If Yes please provide details at 3.2 |

|  |  |  |
| --- | --- | --- |
| 3.2 | If you have answered Yes to any of the above, explain what measures been taken to demonstrate the reliability of the organisation despite the existence of a relevant ground for exclusion? (Self Cleaning) |  |

**Taking Account of Bidders’ Past Performance**

SMC may assess the past performance of a Supplier (through a Certificate of Performance provided by a Customer or other means of evidence). SMC may also assess whether specified minimum standards for reliability for such contracts are met.

In addition, SMC may re-assess reliability based on past performance at key stages in the procurement process (i.e. supplier selection, tender evaluation, contract award stage etc.). Suppliers may also be asked to update the evidence they provide in this section to reflect more recent performance on new or existing contracts (or to confirm that nothing has changed).

**Non-payment of taxes/social security contributions**

SMC reserves the right to use its discretion to exclude a supplier where it can demonstrate the supplier’s non-payment of taxes/social security contributions where no binding legal decision has been taken.

Please note that this section relating to tax compliance only applies where SMC has indicated that the contract is over £5million in value.

“Occasion of Tax Non-Compliance” means:

1. any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 is found to be incorrect as a result of:
   * + 1. a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle;
       2. the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime; and/or
2. the Supplier’s tax affairs give rise on or after 1 April 2013 to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Effective Date or to a penalty for civil fraud or evasion.

|  |  |  |
| --- | --- | --- |
| From 1 April 2013 onwards, have any of your company’s tax returns submitted on or after 1 October 2012; (Please indicate your answer by marking ‘X’ in the relevant box). | | |
| 3.1 | Given rise to a criminal conviction for tax related offences which is unspent, or to a civil penalty for fraud or evasion; | ▢ Yes  ▢ No |
| 3.2 | Been found to be incorrect as a result of:   * + - HMRC successfully challenging it under the General Anti-Abuse Rule (GAAR) or the “Halifax” abuse principle; or     - a tax authority in a jurisdiction in which the legal entity is established successfully challenging it  under any tax rules or legislation that have an effect equivalent or similar to the GAAR or the “Halifax” abuse principle; or     - the failure of an avoidance scheme which the Supplier was involved in and which was, or should have been, notified under the Disclosure of Tax Avoidance Scheme (DOTAS) or any equivalent or similar regime in a jurisdiction in which the Supplier is established. | ▢ Yes  ▢ No |
| If answering “Yes” to either 3.1 or 3.2 above, the Supplier may provide details of any mitigating factors that it considers relevant and that it wishes SMC to take into consideration.  This could include, for example:   * + Corrective action undertaken by the Supplier to date;   + Planned corrective action to be taken;   + Changes in personnel or ownership since the Occasion of Non-Compliance (OONC); or   + Changes in financial, accounting, audit or management procedures since the OONC.   In order that SMC can consider any factors raised by the Supplier, the following information should be provided:   * A brief description of the occasion, the tax to which it applied, and the type of “non-compliance” e.g. whether HMRC or the foreign tax authority has challenged pursuant to the GAAR, the “Halifax” abuse principle etc. * Where the OONC relates to a DOTAS, the number of the relevant scheme. * The date of the original “non-compliance” and the date of any judgement against the Supplier, or date when the return was amended. * The level of any penalty or criminal conviction applied. | | |

**Defining Different Types of Organisations**

The Department for Education is keen to collect information about SMEs. We are particularly interested in discovering how many SMEs apply for our contracts through the tendering process. Completion of the table below is for departmental information purposes only and will have no effect on the evaluation process outcomes. Government is committed to changing how it does business to make sure that small companies, charities and voluntary sector organisations are included and encouraged to compete for our contracts.

A voluntary sector organisation may also be a SME if it has the same attributes.

Defn; A SME must be autonomous, an EU Company not owned or controlled by a non EU parent, and employ less than 250 staff and have sales below €50million

*Source -*http://ec.europa.eu/enterprise/policies/sme/files/sme\_definition/sme\_report\_2009\_en.pdf

Please complete the table below.

|  |  |  |
| --- | --- | --- |
| **Describe your Organisation** | | |
| **What type of supply arrangement best describes you in relation to this bid.** | | **Delete as appropriate** |
| 1. | We are a SME by definition | Yes/No |
| 2. | We are a Charity or Voluntary Sector Organisation (VSO) | Yes /No |
| 3. | We are a mutual organisation | Yes/No |
| 4. | We anticipate using a supply chain to deliver against this service. | Yes/No |
| 5. | We estimate that that our service delivery will be i.e. 40% delivered by VSO’s/SMEs | …….% |
| 6. | If none of the above applies please describe the type of organisation you are: | |
| 7. | Please provide us with your Dun and Bradstreet Number, or a consortium, the lead bidder’s number.  <http://www.dnb.co.uk/dandb-duns-number> |  |

The Department uses Dun and Bradstreet Numbers to manage its data around suppliers; we strongly encourage all suppliers to apply for a free Dunn’s numbers. The link to apply is:-<http://www.dnb.co.uk/myduns> - add ‘GOVERNMENT SUPPLIER’ as a reason for requesting your D&B DUNS number.

Do not delay returning your tender if you do not already have a Dun and Bradstreet number, returning your tender within the deadline is more important.

Declarations

1 ...............................................……………………………. (Name of tenderer) declares that we accept SMC’s standard terms and conditions included at Document 4 Attachment 1 as the basis of the contract; and

2 agree that SMC may disclose the Contractor's information/documentation (submitted to SMC during this Procurement) more widely within Government for the purpose of ensuring effective cross-Government procurement processes, including value for money and related purposes.

3 declare that we have not communicated to any other party the amount or approximate amount of the tender price other than in confidence and for the express purpose of obtaining insurances or a bond in connection with this tender. The tender price has not been fixed nor adjusted in collusion with any third party, and

4 declare that the tender will remain valid until *(insert a date)* and that we are not entitled to claim from SMC any costs or expenses incurred in preparing the tender or subsequent negotiations whether or not the tender is successful.

signed on behalf of the Tenderer ..................................................................................

.

**Attachment 1**

**Terms and Conditions**

****

**Attachment 2**

**Evaluation Criteria**

**Set out in Document 4, Section 2**

**Attachment 3**

**Departmental Security Standards**

1. **Departmental Security Standards for Business Services and ICT Contracts**

|  |  |
| --- | --- |
| “BPSS”  “Baseline Personnel Security Standard” | 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> |
| “CCSC”  “Certified Cyber Security Consultancy” | 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> |
| “CCP”  “Certified Professional” | is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession 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> |
| “CC”  “Common Criteria” | 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. |
| “CPA”  “Commercial Product Assurance”  [formerly called “CESG Product Assurance”] | is an ‘information assurance scheme’ which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards. 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> |
| “Cyber Essentials”  “Cyber Essentials Plus” | Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme.  There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to one of these providers: <https://www.iasme.co.uk/apply-for-self-assessment/> |
| “Data”  “Data Controller”  “Data Processor”  “Personal Data”  “Sensitive Personal Data”  “Data Subject”, “Process” and “Processing” | shall have the meanings given to those terms by the Data Protection Act 1998 |
| "Department’s Data"  “Department’s Information” | is any data or information owned or retained in order to meet departmental business objectives and tasks, including:  (a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are:  (i) supplied to the Contractor by or on behalf of the Department; or  (ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or  (b) any Personal Data for which the Department is the Data Controller; |
| “DfE”  “Department” | means the Department for Education |
| “Departmental Security Standards” | means the Department’s security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver. |
| “Digital Marketplace / GCloud” | 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. |
| “The Commission”  “SMC” | means the Social Mobility Commission |
| “FIPS 140-2” | 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. |
| “Good Industry Practice”  “Industry Good Practice” | means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector. |
| “Good Industry Standard”  “Industry Good Standard” | means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector. |
| “GSC”  “GSCP” | means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: <https://www.gov.uk/government/publications/government-security-classifications> |
| “HMG” | means Her Majesty’s Government |
| “ICT” | means Information and Communications Technology (ICT) is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution |
| “ISO/IEC 27001” “ISO 27001” | is the International Standard for Information Security Management Systems Requirements |
| “ISO/IEC 27002” “ISO 27002” | is the International Standard describing the Code of Practice for Information Security Controls. |
| “ISO 22301” | is the International Standard describing for Business Continuity |
| “IT Security Health Check (ITSHC)”  “IT Health Check (ITHC)”  “Penetration Testing” | means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system. |
| “Need-to-Know” | 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. |
| “NCSC” | 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> |
| “OFFICIAL”  “OFFICIAL-SENSITIVE” | 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.  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 media, as described in the Government Security Classification Policy. |
| “Secure Sanitisation” | 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: <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>  The disposal of physical documents and hardcopy materials advice can be found at: <https://www.cpni.gov.uk/secure-destruction> |
| “Security and Information Risk Advisor”  “CCP SIRA”  “SIRA” | the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also:  <https://www.ncsc.gov.uk/articles/about-certified-professional-scheme> |
| “SPF”  “HMG Security Policy Framework” | 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. <https://www.gov.uk/government/publications/security-policy-framework> |
| ”Tailored Assurance”  [formerly called “CTAS”, or,  ”CESG Tailored Assurance”] | 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. <https://www.ncsc.gov.uk/documents/ctas-principles-and-methodology> |

* 1. The Contractor shall comply with Departmental Security Standards for Contractors which include but are not constrained to the following clauses.
  2. Where the Contractor will provide ICT products or services or otherwise handle information at OFFICIAL on behalf of SMC, the requirements under Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - [Action Note 09/14](https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification) 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, SMC.

12.3 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).

12.3 The Contractor shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements). The ISO/IEC 27001 certification must have a scope relevant to the services supplied to, or on behalf of, SMC. The scope of certification and the statement of applicability must be acceptable, following review, to SMC, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

* 1. 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).
  2. 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 12.14.
  3. 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
  4. 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.
  5. 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.
  6. 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.
  7. 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 12.11 and 12.12 below.
  8. 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.
  9. 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.
  10. Whilst in the Contractor’s care all removable media and hardcopy paper documents containing Departmental Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.
  11. When necessary to hand carry removable media and/or hardcopy paper documents containing Departmental Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This clause shall apply equally regardless of whether the material is being carried inside or outside of company premises.
  12. 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.
  13. 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.
  14. All Contractor or sub-contractor employees who handle Departmental Data must have annual awareness training in protecting information.
  15. 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.
  16. 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.
  17. 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.
  18. 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.
  19. 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.
  20. 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.
  21. 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)