SCHEDULE 2: PART 2 – PERFORMANCE

Drafting note: this Schedule references dates, targets, and Milestones relative to the 2021 Cohort. For all subsequent cohort Call Offs this Schedule will be updated to reflect the relevant Cohort specifics as set out in the Call Off Order.

In this section the words below have the following meaning:

"Department Reporting Template"	means the Department's spreadsheet that will be shared with Contractors post award which will need to be submitted by the 25th of each month.
"Improvement Plan"	means a plan for improvement that the Department can request from the Contractor within ten (10) Working Days in the event of failure.
"KPI"	means the Key Performance Indicators as set out in Annex A of this Schedule.
"Performance Management"	means how the Department will measure the Contractor's performance and progress against the Service Specification (Schedule 1: Part 1), the Contractors Solution (Schedule 1: Part 2), the Implementation Plan (Schedule 7), and Pricing (Annex 1 of Schedule 2: Part 1).
"Performance Manager"	means the person the Contractor will appoint to ensure that the Contract is delivered as specified in the Contract and that Service Levels, Minimum Targets and KPIs are achieved.
"Reporting Period"	means the reporting period that occurs every calendar month from 25th of each month to the 24th of the following month and will commence on the Contract Commencement Date.
"Service Credits"	means the service credits as set out in Table 17 of this Schedule.
"Service Level"	means the Service Levels as set out in Table 16 of this Schedule by which the Contractor's performance will be measured.

1. SERVICE LEVELS AND KPIS

1.1. This section sets out the Service Levels and Key Performance Indicators (KPIs) against which the Parties shall measure the Contractor's performance.

1.2. The objective of the Service Levels and KPIs is to:

1.2.1. ensure that the Services are of a consistently high quality and meet the requirements of the Department;

1.2.2. provide a mechanism whereby the Department can attain meaningful recognition of inconvenience and/or loss resulting from the Contractor's failure to deliver the Services; and

1.2.3. incentivise the Contractor to meet the performance standards and to remedy any failure to meet the required standards expeditiously.

Service Levels

1.3. The Contractor shall ensure compliance with the Service Levels listed in Table 16 (Service Levels).

1.4. The Contractor and the Department shall monitor the Contractor's performance against each of the Service Levels listed in Table 16 (Service Levels).

1.5. The Contractor shall complete and return the monthly Department Reporting Template outlining performance against the Service Levels to date and confirm whether they have been achieved.

1.6. If the Contractor fails to meet any one Service Level in any Reporting Period, the Department reserves the right to apply a Service Credit and take action in line with paragraphs 2.11 to 2.15 (Consequence of Service Failure).

1.7. Service Levels are set out in Table 16 below:

Table 16 Service Levels

Subject	Ref	Service Level	Level to be Achieved
Reporting and Meetings	RM1	Submit to the Department a completed monthly contract management report by the twenty-fifth (25th) of each month using the template provided by the Department.	Submit 100% of monthly contract reports to the Department by 25th of each month.
	RM2	Attend monthly contract management meetings.	100% excluding unavoidable events which prevent attendance.
Administration / Communication	C1	Provide a meaningful response to one hundred per cent (100%) of queries raised by the Department or Service Users and correspondence within three (3) Working Days from the date of receipt or within such other timescales for response as provided specifically for within the terms of the contract. In the event the query raised is complex the Contractor can request an extension of time, which will be subject to agreement by the Department.	100% of responses submitted within three Working Days.
Management Information	MI1	Submit accurate and complete data on Participant and School participation to the Department by the twenty-fifth (25th) of each month. Ensure the data submitted to the Department on this date is reflective of the number of Participants recruited onto the programme at that point in time.	100% of required monthly management information submitted by the 25th of each month.
	MI2	Ensure that all data discrepancies identified by the Department are 100% accurately addressed ahead of the next submission of data. In most circumstances this should be within 28 days of notice.	Resolve 100% of discrepancies by next reporting deadline following notification from the Department.

Finance	F1	Ensure that valid invoices are submitted to the Department by the twenty-fifth (25th) of the month for the relevant Reporting Period.	100% of invoices to be submitted by 25th of the month for the relevant Reporting Period.
	F2	Comply and respond to any requests for Open Book or financial validation data within ten (10) Working Days.	100% of responses made to requests for Open book or financial validation data made within 10 Working Days.
	F3	Ensure that all financial discrepancies identified by the Department are 100% accurately reconciled ahead of the next invoice period and any variances to invoicing values offset.	100% of financial discrepancies accurately reconciled and invoicing values offset by the next Reporting Period deadline following identification or notification of the discrepancy.
Appeals	APP 1	Delivery of an internal process to resolve appeals within three (3) months from the date submitted by the appellant.	100% of the internal processes as defined in the Contractors Appeals Policy to be undertaken within the three (3) month appeal window.
	APP 2	If unresolved within three (3) months from the date submitted by the appellant and all internal processes exhausted, a complete appeal bundle is to be sent to the Department and/or its designated External Body who will act as the final arbiter.	Refer 100% of unresolved appeals for arbitration on expiration of the three (3) month appeal window.
Records and questionnaires	RQ1	All satisfaction questionnaires shall be completed in full and returned to the Department within ten (10) Working Days from the date of completion, and any information requested by the Department shall be provided by the Contractor to the Department within five (5) Working Days from the date of the request.	95% of satisfaction questionnaires to be returned within 10 Working Days from the date of completion and submit 100% of information requested by the department within 5 Working Days.
Design and delivery	D1	Design and delivery of training programmes against the published NPQ Content Frameworks and the Service Requirements set out in the contract.	Meet 100% of Milestone Dates.

	D2	Design and delivery of training programmes against dates and milestones agreed in the Framework Implementation Plan and Call Off Delivery Plans.	Meet 100% of Milestone Dates.
	D3	Iteratively developing the training programme responding constructively to feedback from the Department and External Bodies and meeting deadlines for returning drafts.	Meet 100% of deadlines agreed.
Service Improvement	SI1	Develop a full Continuous Improvement Plan and report progress to the Department against agreed milestones.	Meet 100% of deadlines agreed.
	SI2	Cooperate with the requirements of the QA function by supplying information, facilitating visits, and otherwise supporting the implementation and ongoing work of the QA function.	Respond and comply with to 100% of QA function requirements and requests.
Digital	D1	Digital Service Levels are set out in Annex A of Schedule 1.	As set out in Schedule 1.
Recruitment Service Levels			
Recruitment	R1	Recruit the agreed volume of participants for the NPQ for Leading Teaching.	To have recruited 96% of the agreed recruitment target for Cohort 1 by 25th November 2022 and 96% of the overall recruitment target (which is the sum total of Cohort 1 and Cohort 2) by 10th March 2023. Table 20 of Annex A, Schedule 2 Part 2 sets out the measures used to monitor performance
	R2	Recruit the agreed volume of participants for the NPQ for Leading Behaviour and Culture.	
	R3	Recruit the agreed volume of participants for the NPQ for Leading Teacher Development.	
	R4	Recruit the agreed volume of participants for the NPQ for Senior Leadership.	
	R5	Recruit the agreed volume of participants for the NPQ for Headship.	
	R6	Recruit the agreed volume of participants for the NPQ for Executive Leadership.	
	R7	Recruit the agreed volume of participants for the NPQ for Early Years Leadership.	
	R8	Recruit the agreed volume of participants for the NPQ for Leading Literacy.	

KPIs

1.8. The Parties shall monitor the Contractor's performance against each of the KPIs listed in Annex A of this Schedule (KPIs) at agreed intervals to be confirmed at contract award.

1.9. If at the agreed reporting milestone, the Contractor:

1.9.1. achieves a KPI rating of 'Good' then the performance measure will be achieved, and no further action will be required;

1.9.2 achieves a KPI rating of 'Approaching Target' then the performance measure will not be achieved, but no further action will be required;

1.9.2. achieves a KPI rating of 'Requires Improvement' or 'Inadequate', then the performance measure will not be achieved and it will be declared a 'Service Failure' and notwithstanding the provision of clause 1.4 (Annex 2 to Schedule 2: Part 1), the Department reserves the right to apply a Service Credit and take action in line with paragraphs 2.11 to 2.15 (Consequence of Service Failure) of this Schedule.

1.10. In line with the cross-government transparency agenda the Department reserves the right to make the Contractor's performance against the KPIs in Annex A of this Schedule available in the public domain, which may include publishing them on gov.uk and including them in any related transparency reporting.

2. PERFORMANCE MANAGEMENT

2.1. The Department shall monitor the Contractor's performance and progress against the Service Specification (Schedule 1: Part 1), the Contractor's Solution (Schedule 1: Part 2), the Implementation Plan (Schedule 7), and Pricing (Annex 1 of Schedule 2: Part 1) within a Reporting Period and during performance review meetings. The Contractor shall cooperate with the Department in this regard and provide any information and evidence reasonably required by the Department within five (5) Working Days of a request being received.

2.2. The Contractor shall appoint a named Performance Manager who will cooperate with the Department to ensure that the Services are delivered as specified in the Contract and that Service Levels, Minimum Targets and KPIs are achieved.

2.3. The purpose of the performance review meetings is to encourage an open and regular dialogue between the Parties. The Parties shall review performance, discuss opportunities for continuous improvement, and address any complaints or persistent problems encountered.

2.4. Performance reviews shall be documented. The Contractor shall provide any information and data requested by the Department to facilitate the reviews and arrange, where necessary, access to any of Contractor Premises or delivery locations, including those operated by Sub-Contractors.

2.5. The Department may instruct the Contractor to take appropriate remedial action where the Department reasonably considers that the Implementation Plan and/or a Performance Improvement Plan is not being complied with, and the Contractor shall take such remedial action.

2.6. If there is a failure to achieve a Service Level, Minimum Target or KPI, the Contractor shall use all reasonable endeavours to immediately minimise the impact of any failure and to prevent such a failure from recurring.

2.7. The Contractor shall ensure that all systems and processes used for the monitoring and recording of performance are robust.

Contractor Management Information (MI) Requirements

2.8. The Department intends to design, build, host, and manage a central Digital Platform that Contractors can use to present online course content for Participants and collate Management Information from Contractors. For contingency purposes only the Department will require the Provider to collect Participant and School data using a spreadsheet developed by the Department (please refer to the management information and digital requirements as set out in the Service Specification for more detail).

2.9. The Contractor shall supply Management Information and Data relevant to the delivery of the Services to the Department, using formats and to timescales as detailed in the Specification or as are otherwise notified to the Contractor by the Department.

2.9A In addition to the provision of Management Information, the Contractor shall respond to and provide additional information (at no additional charge) relating to the provision of the Services as required by the Department from time to time.

2.10. The Department shall be entitled to amend the Reporting Period and format in respect of any or all Management Information or waive the requirement for any aspect of the Management Information to be reported upon by giving the Contractor not less than one (1) Months' notice in writing.

Consequence of Service Failure

2.11. With the exception of Service Levels for Recruitment, where the Service Failure is a result of the Contractor failing to meet any one Service Level by the dates set out in Table 16 of Schedule 2 Part 2 the Contractor must agree and implement a plan to rectify the Service Failure within agreed timescales. where the Service Failure is as a result of the Contractor failing to meet any one Service Level by the dates set out in Table 16 of Schedule 2 Part 2 for two consecutive Monthly Reporting Periods, and the Contractor has not addressed and resolved the Service Level failure within the time agreed between the Contractor and the Department, the Department will apply a Service Credit.

2.12. Where the Service Failure is as a result of the Contractor failing to meet one or more of Service Levels that relate to Recruitment by the dates set put in Table 16 of Schedule 2 Part 2, the Contractor must agree and implement a plan to rectify the Service Failure within agreed timescales. If the Contractor fails to address and resolve the Service Level Failure relating to Recruitment within the timescales agreed the Department may apply a Service Credit at its discretion.

2.13. Without prejudice to any other rights or remedies arising under this Contract, including under clause 10 (Termination) for material breach, if the Contractor incurs a Service Failure in any Relevant Period, the Contractor acknowledges and agrees that the Department shall have the right to exercise (in its absolute and sole discretion) all or any of the following remedial actions:

2.13.1. The Department shall be entitled to require the Contractor, and the Contractor agrees to prepare and provide to the Department, a plan for improvement (an "Improvement Plan") within ten (10) Working Days of a written request by the Department for such Improvement Plan. Such Improvement Plan shall be subject to the Department's prior approval and the Contractor will be required to implement any approved Improvement Plan, as soon as reasonably practicable;

2.13.2. The Department shall be entitled to require the Contractor, and the Contractor agrees to attend, within a reasonable time one (1) or more meetings at the request of the Department in order to resolve the issues raised by the Department in its notice to the Contractor requesting such meetings;

2.13.3. The Department shall be entitled to serve a notice of improvement ("Improvement Notice") on the Contractor and the Contractor shall implement such requirements for improvement as set out in the Improvement Notice;

2.13.4. The Department shall be entitled to issue interim performance measures and/or milestones in order to monitor the Contractors implementation of any Improvement Plan or Improvement Notice;

2.13.5. If not already applied to the Service Failure prior to this point, apply a Service Credit.

2.14. In the event that the Department has, in its absolute and sole discretion, invoked one or more of the remedies set in paragraph 2.11 and 2.12 above the Department may suspend the Contractor from the Framework Agreement pending the Department being satisfied that the Contractor has;

2.14.1. implemented the requirements for improvement set out in the Improvement Notice; and/or

2.14.2. implemented an Improvement Plan approved by the Department; and/or

2.14.3. met the interim performance measures and/or milestones.

2.15. Whether or not the Department has exercised its rights under pursuant to paragraph 2.13 in the event that the Department has, in its absolute and sole discretions invoked one or more of the remedies set out in paragraph 2.12 above and allowed the Contractor reasonable opportunity to remedy the Service Failure, and the Contractor either;

2.15.1. fails to implement such requirements for improvement as set out in the Improvement Notice; and/or

2.15.2. fails to implement an Improvement Plan approved by the Department; and/or

2.15.3. fails to meet the interim performance measures and/or milestones, then (without prejudice to any other rights and remedies of termination provided for in this Contract), the Department shall be entitled to terminate this Contract and with immediate effect by notice in writing in accordance with clause 10.5. Termination of the Contract will be considered a Material Default and the Department may at its absolute discretion terminate the Framework Agreement as per paragraph 7.4 of the Framework Agreement.

3. SERVICE CREDITS

3.1. Accrual of Service Credits shall entitle the Department to a reduction in the Charges.

3.2. Financial consequences of Service Credits will be calculated against the Total Contract Value. The Contractor shall off-set the value of any Service Credits against the Charges for the Contract up to a maximum of 5% of the Total Contract Value.

3.3. The Contractor confirms that it has taken Service Credits and the potential financial consequences into account in calculating the Charges. Both Parties agree that the Service Credits are a reasonable method of adjusting the Charges to reflect failure to meet minimum performance standards.

3.4. The financial consequences that will be applied in the event of a Service Credit are broken down in Table 17 below.

Table 17: Service Credits

Service Credits accrued:	Financial consequence equivalent to:
1 Service Credit	1% of Call Off Contract Value
2 Service Credits	2% of Call Off Contract Value
3 Service Credits	3% of Call Off Contract Value
4 Service Credits	4% of Call Off Contract Value

5 or more Service Credits	5% of Call Off Contract Value

4. SET UP MILESTONES (ONLY APPLIES TO SET UP CALL OFF)

4.1. Contractor's that are awarded Set Up Call Off Contracts are required to achieve the Milestones set out in Table 18 and 19 below:

Table 18 Milestones for Set Up (Lot 2)	
Milestone	**Deadline for Milestone to be achieved**
Lot 2 Milestone 1: Provider Implementation Plan agreed.	w/c 18 April 2022
Lot 2 Milestone 2: Sample content shared for quality review and approved by the Department.	w/c 12 September 2022
Lot 2 Milestone 3: Host a User Digital Platform and complete integration with the Department's Digital platform.	w/c 30 June
Lot 2 Milestone 4: Further reassurance of the quality of content to the satisfaction of the Department.	w/c 19 December 2022
Lot 2 Milestone 5: All final curriculum content for six NPQs and all Summative Assessment materials submitted to the Department.	w/c 13 March 2023

Table 19 Milestones for Set Up (Lot 3)	
Milestone	**Deadline for Milestone to be achieved**
Lot 3 Milestone 1: Provider Implementation Plan agreed.	w/c 18 April 2022
Lot 3 Milestone 2: Sample content shared for quality review and approved by the Department.	w/c 12 September 2022
Lot 3 Milestone 3: Host a User Digital Platform and complete integration with the Department's Digital platform. (NB. Only for Providers who are not delivering a Lot 2 Set Up Call Off Contract)	w/c 30 June

Lot 3 Milestone 4: Further reassurance of the quality of content to the satisfaction of the Department.	w/c 19 December 2022
Lot 3 Milestone 5: All final curriculum content for the 2 NPQs and all Summative Assessment materials submitted to the Department.	w/c 13 March 2023

4.2. Time is of the essence in relation to Milestone 4 and so the failure to achieve the relevant Milestone by the Milestone Date will entitle the Department to terminate the Set Up Call Off Contract for Serious Breach which cannot be remedied in accordance with clause 10.5.1.

4.3. At each Milestone deadline specified in Table 18 and 19 above, the Department will assess if the Contractor has achieved the Milestone. If the Contractor has not achieved the Milestone, the Department reserves the right to apply any or all of the following:

4.3.1. immediately require the Contractor to stop or not start any part of the Services;

4.3.2. require the Contractor to;

4.3.2.1. revise and resubmit their Implementation Plan;

4.3.2.2. reschedule any activity;

4.3.2.3. attend meetings with the Department and/or its QA Function, submit reports, report on progress, provide additional resources and take the necessary action to provide assurances to the Department that the failure to achieve the Milestone will not adversely affect the Services or other Call Off Contracts that the Contractor is currently delivering;

4.3.3. treat the failure to achieve the Milestone as a Service Failure and apply the rights set out in paragraph 2.11 to 2.15 of this Schedule and impose revised deadlines on the Milestones;

4.3.4. treat the failure to meet the Milestone as a Serious Breach and apply clauses 10.3 or 10.5.1;

4.3.5. recover any Set Up Fees already paid to the Contractor.

5. SET UP MILESTONES (ONLY APPLIES TO DELIVERY CALL OFFS AWARDED WHILST THE CONTRACTOR'S SET UP CALL OFF CONTRACT IS STILL BEING DELIVERED)

5.1. If the Contractor's fails to achieve any of the Milestones included in a Set Up Call Off Contract but at the same time is delivering the Services under a Call Off Contract other than a Set Up Call Off Contract the Department reserves the right to apply any or all of the following in relation to the said Call Off Contract:

5.1.1. immediately require the Contractor to stop or not start any part of the Services, including delaying the Cohort Commencement Date;

5.1.2. require the Contractor to;

5.1.2.1. revise and resubmit their Delivery Plan and Implementation Plan;

5.1.2.2. reschedule any activity;

5.1.2.3. attend meetings with the Department and/or its QA Function, submit reports, report on progress, provide additional resources and take the necessary action to provide assurances to the Department that the failure to achieve the Milestone will not adversely affect the Services;

5.1.3. treat the failure to meet the Milestone as a Serious Breach and apply clauses 10.3 or 10.5.1;

5.2. Time is of the essence in relation to Milestone 4 included in the Set Up Call Off Contract and so the failure to achieve that Milestone Date will also entitle the Department to terminate this Contract for Serious Breach which cannot be remedied in accordance with clause 10.5.1.

5.3. In the event the Department terminates this Call Off Contract in accordance with paragraph 5.1.3 of this Schedule, the Contractor shall assist and support the Department to ensure an orderly and smooth transfer of Participants to other contractors or providers.

ANNEX A TO SCHEDULE 2: PART 2 – KEY PERFORMANCE INDICATORS

1.1. The KPIs in Table 20 set out the measures the Department will use to monitor the Contractor's performance. The KPIs will be applied to each Call Off Contract, with the Cohort specific targets and milestones included in the Call Off Contract in Part 2 of Schedule 2.

1.2. The Department and Schools reserve the right to tailor, amend or add additional KPIs to those stated in Table 20, and define the KPIs for Future Services, for Call Off Contracts to ensure they reflect the needs and requirements of the specific Cohort.

Rating	Criteria	Performance Management
Good	The supplier is meeting or exceeding the KPI target	N/A
Approaching Target	The supplier is close to meeting the KPI target	N/A
Requires Improvement	The performance of the supplier is below that of the KPI target	Improvement Plan with a suspended Service Credit
Inadequate	The performance of the supplier is significantly below that of the KPI target	Service Failure – Improvement Plan and Service Credit applied.

Table 20: Key performance indicators		
KPI	**Measure**	
1 – Recruitment Recruit the target number of participants with a completed Start Declaration (by output 1 review point specified in Schedule 2: Part 1, para 13.2, Table 6 for Specialist NPQs and Table 7 for Leadership NPQs) on the Department's digital registration service, for each of the Cohort commencement dates. Performance reviewed monthly with final monitoring target date agreed at call off stage.	**Recruitment % against target:**	
	Good	96% +
	Approaching Target	90% - 95%
	Requires Improvement	75% - 89%
	Inadequate	Below 75%
2 – Quality Assessment The accuracy level of Summative Assessments undertaken by participants completing NPQ's, within the Call off Contract windows. Monitoring, linked to the completion of Content Quality Review via the Quality Management System which shall be immediately submitted, and accessible, to the Department and its QA function upon request.	**Accuracy level at Summative Assessment:**	
	Good	95% +
	Approaching Target	93% - 94%
	Requires Improvement	90% - 92%
	Inadequate	Below 90%
3 – Retention The number of Participants that start the training retained at the end of year 2 of delivery. Performance reviewed monthly and reported at end of years 1 and 2 of the programme.	**Retention rate:**	
	Good	85% +
	Approaching Target	80% - 84%
	Requires Improvement	70% - 80%
	Inadequate	Below 70%
3 – Satisfaction	**Rate of participants rating the experience as 'Good' or better:**	

The number of Participants who rate the training as 'Good' or better. The DfE will design a survey to be issued to participants via the Lead Provider. Minimum response rate of 40% required. Surveys will be issued and performance measured at the end of years 1 and 2 of the programme.	**Good**	80% +
	Approaching Target	75% - 79%
	Requires Improvement	70% - 74%
	Inadequate	Below 70%

SCHEDULE 3: ADDITIONAL CLAUSES

1. Departmental Security Standards

"BPSS" "Baseline Personnel Security Standard"	a level of security clearance described as preemployment 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 Contractors 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-cyberconsultancy
"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/certifiedprofessional
"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/commercialproduct-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”	shall have the meanings given to those terms by the GDPR.
“Data Controller”	
“Data Processor”	
“Personal Data”	
“Sensitive Personal Data”	
“Data Subject”, “Process” and “Processing”	
"Department’s Data"	is any data or information owned or retained in order to meet departmental business objectives and tasks, including:
“Department’s Information”	(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;
“Department”	means the Department for Education.
“Department”	
“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.
“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.
General Data Protection Regulation (GDPR)	replaces Data Protection Act clauses for use in contracts that are live on or after 25th May 2018.
“Good Industry Practice”	means the exercise of that degree of skill, care,

“Industry Good Practice”	prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
“Good Industry Standard”	this means the implementation of products; and
“Industry Good Standard”	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”	means the Government Security Classification.
“GSCP”	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)”	means an assessment to identify risks; and
“IT Health Check (ITHC)”	vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity
“Penetration Testing”	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 Department 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/securesanitisation-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-certifiedprofessional-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 Departments procuring IT systems, products and services, ranging from simple software components to national infrastructure networks. https://www.ncsc.gov.uk/documents/ctas-principlesand-methodology

1.1. The Contractor shall comply with Departmental Security Standards for Contractors, which include but are not constrained to the following clauses;

1.2. As the Contractor will be handling 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. 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.

1.6. 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.

1.7. 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 1.8 to 1.11 below.

1.8. 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.

1.9. 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.

1.10. 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.

1.11. 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.

1.12. 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.

1.13. 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.

1.14. All Contractor or Sub-Contractor employees who handle Departmental Data must have annual awareness training in protecting information.

1.15. 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 Contractor 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.

1.16. 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.

1.17. 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.

1.18. 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.

1.19. The Department reserves the right to audit the Contractor or Sub-Contractors providing the Services 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.

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

1.21. 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 Department 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 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).