Number	Question	Max. available score
Technical Question 3 – Mobilisation and Resource Capacity	*Please set out your strategy for mobilising your resources at pace both early in the programme and flexing as required to meet programme demand.* *Your response should include:* - *Clear evidence and rationale to support your approach.* - *Approach to recruitment and staffing arrangements* - *Associated time and organisational considerations.* *(max. 500 words)*	10

Tender response:

We've supported school leaders via peer-to-peer groups and 1:1 telephone counselling for over 20 years, including the DfE school leaders' pilot since Aug 2020. We're uniquely positioned to increase service provision immediately.

Resources, and delivery mechanisms, already exist. The pilot evaluation provides evidence of the success of our approach. With minor improvements, we're ready to scale up, without the need for lengthy handover processes.

Early in the programme:

We've a team in place and can mobilise immediately:

- Our Programme Manager is responsible for mobilisation, allocating 100% of her time. She is supported by Director of Programmes, who'll allocate 40% of her time. Both delivered the pilot service.
- Our Operations Manager, and Service Delivery team, will provide additional resource support. We'll allocate 50% of their time during mobilisation.
- Our Communications team is ready to start promotion. We have key messages, social media assets and a range of marketing tools, with proven effectiveness.
- We're ready to promote the service from day one and can reach school leaders at the start of the new school year.
- Our team includes 18 Associates. All meet the qualification criteria, are trained, and can start peer-to-peer delivery immediately.

- We also have 12 supervision Associates who'll work with our existing processes and can begin delivery immediately.
- Our existing sub-contractor Workplace Options (WPO) will deliver one-to-one counselling. Resources and processes are in place, providing a smooth transition into the new phase.
- Our CEO is accountable to the Board for our success. She'll remain close to the team throughout.

We have the infrastructure to mobilise quickly:

- We established infrastructure, processes and technology to deliver successfully during the pilot. We can test and refine the service, as we start from a base of strong understanding.
- Participant journeys are established for both peer-to-peer and 1:1 support. We'll base additional activity on them, making improvements from day one.

Flexing to meet programme demand:

- We have capacity to comfortably deliver this programme, but from the pilot, we understand where flexibility is needed.
- During the pilot, the peer-to-peer service was oversubscribed so we increased capacity to deliver additional groups via Associates. Our supervision Associates will do the same.
- If necessary, we'll continue to grow our Associate team. Robust recruitment processes are in place. We've proven models for forecasting Associates' capacity, which worked successfully during the pilot.
- We'll implement a guided self-selection tool allowing school leaders who meet selection criteria to register for the most appropriate support.
- WPO employ over 250 accredited counsellors, allowing them to meet fluctuating demand. Monthly resourcing meetings allow us to forecast demand and plan resources effectively.
- Programme promotion is a priority. In addition to ongoing communications activity, our team will reprioritise and focus on programme promotion if required.
- Reaching school leaders is core to our mission. We're committed to flexing internal resourcing to increase capacity.
- We'll recruit a Senior Programme Officer, who'll support delivery of the programme, overseen by our Programme Manager.

Technical Question that Tenderers need to respond to		
Number	**Question**	**Max. available score**
Technical Question 4 – Programme Evaluation	*Please set out your approach for evaluation of the programme, including but not limited to; capturing lessons learned, evaluating impact and ensuring opportunities for continuous improvement.* *Your response should include:* - *Clear evidence and rationale to support your approach.* - *Details of approach and processes for monitoring progress against SLAs, milestones and KPIs.* - *Details of how you will collect and process sufficient feedback, learn lessons and ensure opportunities for continuous improvement are implemented.* *(max. 500 words)*	10
Tender response:		

Delivering the DfE school leaders' pilot, and similar services across Wales, provides us unique insight into evaluation of this programme.

Our evaluation and monitoring team will be: our Programme Manager, supported by Director of Programmes and Research Projects Manager who has 17 years' experience in research and evaluation in the education sector.

Progress against SLAs, milestones and KPIs

We're committed to honest and transparent communication with partners. Our Director of Programmes and CEO are PRINCE2 qualified, with extensive experience in monitoring largescale programmes against SLAs, milestones and KPIs.

Mobilisation

- We'll develop reporting templates to track against SLAs, milestones and KPIs including an internal progress report.

- Programme KPIs will be added to our KPI dashboard. It is regularly reviewed by our CEO, Leadership and Trustees.
- We already have processes in place for Associates and our subcontractor, Workplace Options (WPO), to provide information on number of sessions delivered. We tested these during pilot and are confident they're fit for purpose.

Delivery

- We'll hold monthly internal progress meetings to discuss risks and troubleshoot issues.
- We'll complete an internal monthly progress report and take a RAG rating approach, with risks having a designated owner and mitigations.
- We'll hold monthly resource meetings with WPO to ensure they're on track.
- WPO will provide weekly reports on counselling sessions. They'll implement a "call-back" service so participants can re-schedule sessions, supporting completion rates.
- Associates will update our secure database once beneficiary sessions are delivered, allowing us to track progress live.

Sufficient feedback, lessons learnt and opportunities for continuous improvement.

- We have an established set of evaluation metrics for peer-to-peer and one-to-one support, which will form our baseline.
- We'll ask a series of pre and post questions for each service, including WEMWBS[10] for measuring participants' wellbeing.
- Our secure system will automatically send questionnaires and collate responses.
- Participant feedback questions include: experience of signing up, quality of delivery, experience of associates and impact measurements.
- We'll review feedback monthly and include within the progress report, with recommendations for continuous improvements.
- All supervisors, counsellors and facilitators will have regular supervision: a space for them to reflect on their practice.
- We'll host meetings for Associates to share feedback, discuss lessons learned and share best practice. This shared learning has been invaluable during the pilot. We'll do the same for our supervision Associates.
- We'll hold monthly resourcing meetings with WPO and quarterly review sessions with their clinicians to receive feedback and provide ongoing review.
- We'll hold a conference for the full delivery team to come together and share learning, best practice and identify improvements.
- Our Director of Programmes will produce a monthly vlog, updating all colleagues on progress and learning.
- We'll produce impact reports throughout the programme, to complement the independent external evaluation. The reports will provide insights for DfE on programme delivery, and recommendations for future approaches.
- We welcome an independent external evaluation, having seen the benefits of this during pilot phase.

[1] https://warwick.ac.uk/fac/sci/med/research/platform/wemwbs/using/howto/

Number	Question	Max. available score
Social Value Question 1 - Improvements to Workplace Conditions	*Please set out the measures you will take during the Contract Period to deliver improvements to workplace conditions that support the COVID -19 recovery effort including effective social distancing, remote working, and sustainable travel solutions.* *Your response should include activities that demonstrate and describe your existing or planned:* *1 Understanding of the need for improvements to workplace conditions that support the COVID-19 recovery effort including effective social distancing, remote working, and sustainable travel solutions.* *2 Engagement plans to engage the contract workforce in deciding the most important workplace conditions to address.* *3 Actions to improve contract workplace conditions that support the COVID-19 recovery effort including those worst affected or who are shielding. Illustrative examples: effective social distancing; remote and flexible working; sustainable travel solutions; opportunities and expectations of staff training; and awareness raising on health and wellbeing for the contract workforce, including around loneliness and isolation caused by COVID-19.* *4 Methods to measure staff workforce conditions over time and adapt to any changes in the results, with clear processes for acting on issues identified.* *Please upload Tenders* ***Annex H - SV project plan 1*** *to support this response.* *)*	5
Tender response:		
Since the COVID-19 outbreak we've taken measures to improve workplace conditions. We've made improvements for our own workforce, and adapted our service provision to support the COVID -19 recovery effort for education staff. We're committed to continuing this.		

Understanding the need for improvements:

Our workforce:

- We continue to follow Government guidelines, with our Director of Finance and Operations holding responsibility for office safety. This includes ongoing safety precautions, social distancing, office attendance rota, daily cleaning and regular communications with staff.
- From September, we'll pilot a new blended working approach. Whilst we recognise the benefits flexible working brings, we retain an explicit commitment to relational working. We encourage people to meet in person, understanding the positive impact this can have on personal wellbeing and relationships.
- We'll continue to offer flexible working so that staff can avoid travelling during peak hours.
- We'll continue to review the needs of those working from home, ensuring they have access to adequate equipment and support. We're committed to improving working conditions for staff at home and at the office.

Education workforce:

- We'll continue to deliver our services remotely, including peer-to-peer and 1:1 support. We'll continue to invest in IT solutions so that participants can access our services safely.
- We've published a range of information, guidance and advice to support the wellbeing of education staff, including advice on improving workplace conditions both in response to Covid-19 and more generally. We'll publish further resources.

Engaging the workforce in deciding the most important workplace conditions to address:

Our workforce:

- Implement blended working model and encourage staff feedback.
- Staff surveys and pulse surveys to inquire how we can further improve workplace conditions. We always share results with staff and involve them in development planning.
- CEO meetings with every team member each year to offer a "safe" space for issues to be raised outside of line management relationships.
- Regular meetings with the Associate team to share technical learning, but also to raise any organisational issues.
- Support for Associates to assist them with adopting remote practices.
- Surveys / group discussions with Associates to inform decision-making. We work in partnership with Associates e.g. they were heavily involved in co-designing our peer support service.

Education workforce:

- We'll engage the workforce via our 2021 Teacher Wellbeing Index to understand key issues around workplace conditions. We'll make and monitor improvement recommendations.
- We're setting up reference groups with target beneficiaries (outside this project) which can offer school leader perspectives on this programme, as well as workforce issues.

Actions to improve contract workplace conditions that support the COVID-19 recovery:

Our workforce:

- Carrying out risk assessments, including for staff who are worst affected or who are shielding. Also carrying out stress risk assessments, understanding the long-term impact of COVID-19 on personal mental health.
- Piloting blended working. Those who need to shield will work from home where needed, supported by adequate equipment.
- We'll run workshops for all staff on how to look after their own wellbeing.
- We'll invest in further line management training, including supporting wellbeing, during the contract period.
- All staff are encouraged to complete a wellbeing action plan, highlighting how workplace conditions may affect their mental and physical health.
- Induction for new staff includes in person meetings with supportive colleagues, or Zoom mentoring, as appropriate.

Education workforce:

- Hosting regular webinars for school leaders, raising awareness of how they can prioritise their own wellbeing alongside guidance on improving workplace conditions. We'll support school leaders to create psychologically safe workplaces post-COVID-19.

Methods to measure staff workforce conditions:

Our workforce:

- Staff surveys and pulse surveys to check in and to inquire about how we can further improve staff wellbeing. Full results are shared with staff. They have the opportunity to feed into resulting development plans.
- In our governance structure we have a Trustee committee that looks at our people strategy and staff feedback. This mechanism holds the leadership team to account for the wellbeing of staff.
- Our strategic plan is explicit about the importance of our people and our annual delivery plan includes specific actions to continuously improve our culture and processes around workforce support.

Education workforce:

- Our Teacher Wellbeing Index is published in Nov 2021 with recommendations we'll monitor.

Number	Question	Max. available score
Social Value Question 2 - Health and Reduced Demand on Public Services	*Please set out the measures you will take during the Contract Period to deliver support for the physical and mental health of people affected by COVID-19, including reducing the demand on health and care services.* *Your response should include activities that demonstrate and describe your existing or planned:* 1 *Understanding of the level of participation by organisations to drive business creation and growth, especially in the context of COVID-19 where new ways of working are needed to deliver services.* 2 *Plans to engage the contract workforce in deciding the most important issues to address and description of how the organisation will respond to and monitor delivery of the agreed actions.* 3 *Inclusive and accessible recruitment practices, development practices and retention-focussed activities including those provided in the Guide for line managers on recruiting, managing and developing people with a disability or health condition.* 4 *Actions to invest in the physical and mental health[1] and wellbeing of the contract workforce, especially in the context of COVID-19, including reducing the demand on health and care services. Illustrative examples: implementing the 6 standards in the Mental Health at Work commitment; where appropriate implementing the mental health enhanced standards, for companies with more than 500 employees, in Thriving at Work with*	5

	respect to the contract workforce, not just 'following the recommendations'; staff training and awareness raising on health and wellbeing for the contract workforce, including around loneliness. 5 *Methods to measure staff physical and mental health and wellbeing engagement over time and adapt to any changes in the results.* 6 *Commitment to report publicly on the health and wellbeing of staff comprising the contract workforce (including the supply chain), following the recommendations in the Voluntary Reporting Framework, with clear processes for acting on issues identified.* *Responses to this question should be provided using* ***SVQ2 – Social Value Response Document*** *Please upload as* ***Annex I – SV project plan 2*** *to support this response.*	

Tender response:

Social value is at the heart of everything we do at Education Support. We're the only UK charity dedicated to improving the mental health and wellbeing of education staff. Our research shows this workforce is negatively impacted by COVID-19.[11]

Every day, our work reduces demand on health and care services. In 2020/21 we gave 9,570 education staff access to BACP accredited counsellors via our helpline, reducing demand on the NHS. Q1 2021/22, has seen a 34% use increase compared to the same period last year. We'll continue providing this support during the contract period, supporting beneficiaries to access counselling.

We provide grants to those working in education who are experiencing financial problems caused by COVID-19, including unemployment or ill health.

We'll drive business growth through our provision of professional supervision via trusted Associates. This also drives new ways of working (and capacity) in the sector, as professional supervision is not yet widely used in education, despite evidence of its effectiveness.

We'll continue working in new ways, delivering our services remotely online/by telephone, helping us to reach more people and further reduce demand on health and care services.

We'll engage our workforce, and wider education workforce, in deciding important issues:

Our workforce:

[11] https://www.educationsupport.org.uk/sites/default/files/resources/covid-19_and_the_classroom.pdf

- A key issue is 'return to work' post COVID-19. We'll pilot blended working to support staff to safely return to the office.
- We'll regularly meet our delivery team (Associates and sub-contractor) to understand delivery and COVID-19 issues impacting participants. We'll use the feedback to refine service delivery.
- We'll provide supervision, regular learning sessions and group conferences to allow engagement with the delivery team.

Education workforce:

- We'll engage the workforce via our 2021 Teacher Wellbeing Index to understand key issues and make recommendations that we'll monitor.
- We'll review helpline data to understand the issues affecting people due to COVID-19 and deliver support to respond.
- We're establishing education sector reference groups (beyond this project) which will give insight into school leader views on our services, including this one.

We prioritise open and accessible recruitment practices, actively promoting opportunities through diverse networks. We have a variety of policies to support staff physical and mental health needs. We're quick to make reasonable adjustments to support staff to work in ways that suit them and are committed to continuing this. We'll also explore becoming a Disability Confident employer.

Physical and mental wellbeing is central to our work. We exist to support the education workforce and this project does that. We role model positive employment practices in line with the Mental Health at Work (MHAW) commitment e.g. explicit investment in creating a supportive culture, prioritising staff mental health, providing tools and support.

Our workforce:

- We're a MHAW commitment signatory. Our Director of Programmes developed the commitment on behalf of the Thriving at Work Leadership Council, of which she is a member. She is leading implementation of the standards internally.
- We'll encourage our sub-contractor to sign the commitment and support them to implement it.
- We hold staff wellbeing workshops, including for line-managers, and will continue to do so.
- Staff have access to our Employee Assistance Programme, including BACP accredited counselling. This reduces the demand on mental health services.
- Our Associates and counsellors will receive professional supervision giving them space to reflect and receive support.

Wider education workforce:

- We recently tailored the MHAW commitment standards for the education sector, for our Taking Care of Teachers Hub. We provide schools with tools to implement the standards, helping them prioritise staff mental health and wellbeing and will continue to do so.
- We'll develop information around loneliness for education staff, drawing on our expertise.

We'll use various methods to measure staff physical and mental health:

Our workforce:

- Staff and pulse surveys to check how we can further improve staff wellbeing; results shared with staff. They have the opportunity to feed into resulting plans.
- Questions around physical/mental health as part of monthly 1:1 meetings.
- CEO meetings with every team member each year to offer a space for issues to be raised.
- Internal and external wellbeing training provision, e.g. Mental Health First Aid training.

Education workforce:

- Our Teacher Wellbeing Index is published in Nov 2021 with recommendations we'll monitor.

As a small organisation, we've not reported on our workforce externally. Our internal reporting includes full transparency with our Board of Trustees (e.g. sharing details of staff surveys including qualitative comments). Over the coming year, we'll revisit what we can do externally to increase transparency.

750 words.

Schedule 11

Data Handling and Systems Assurance (Security)

Definitions

12. Departmental Security Standards for Business Services and ICT Contracts

"BPSS" "Baseline Personnel Security Standard"	means the Government's HMG Baseline Personal Security Standard . Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard
"CCSC" "Certified Cyber Security Consultancy"	is the National Cyber Security Centre's (NCSC) approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. 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. See website: https://www.ncsc.gov.uk/information/about-certified-professional-scheme
"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.. 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 these providers: https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body

"Data" "Data Controller" "Data Protection Officer" "Data Processor" "Personal Data" "Personal Data requiring Sensitive Processing" "Data Subject", "Process" and "Processing"	shall have the meanings given to those terms by the Data Protection Act 2018
"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 / G-Cloud"	means the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects.
End User Devices	means the personal computer or consumer devices that store or process information.
"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) and 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"	means the Need-to-Know principle 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) 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). the term 'OFFICIAL–SENSITIVE 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 GSCP.
"RBAC" "Role Based Access Control"	means Role Based Access Control. A method of restricting a person's or process' access to information depending on the role or functions assigned to them.
"Storage Area Network" "SAN"	means an information storage system typically presenting block based storage (i.e. disks or virtual disks) over a network interface rather than using physically connected storage.
"Secure Sanitisation"	means the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. NCSC Guidance can 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"	means 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
"Senior Information Risk Owner" "SIRO"	means the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for overseeing the management of information risk across the organisation. This includes its executive agencies, arms length bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties.

"SPF" "HMG Security Policy Framework"	means 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

12.1. The Contractor shall be aware of and comply the relevant HMG security policy framework, NCSC guidelines and where applicable DfE Departmental Security Standards for Contractors which include but are not constrained to the following clauses.

- (Guidance: Providers on the HMG Digital Marketplace / GCloud that have demonstrated compliance, as part of their scheme application, to the relevant scheme's security framework, such as the HMG Cloud Security Principles for the HMG Digital Marketplace / GCloud, may on presentation of suitable evidence of compliance be excused from compliance to similar clauses within the DfE Security Clauses detailed in this section (Section 12).)

12.2. Where the Contractor will provide products or services or otherwise handle information at OFFICIAL for the Department, the requirements of Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - Action Note 09/14 dated 25 May 2016, or any subsequent updated document, are mandated, namely that contractors supplying products or services to HMG shall have achieved, and will be expected to retain Cyber Essentials certification at the appropriate level for the duration of the contract. The certification scope shall be relevant to the services supplied to, or on behalf of, the Department.

- (Guidance: Details of the acceptable forms of equivalence are stated at Section 9 of Annex A within the link to Cabinet Office document in this clause).
- (Guidance: The Department's expectation is that the certification scope will be relevant to the services supplied to, or on behalf of, the Department. However, where a contractor or (sub) contractor is able to evidence a valid exception or certification to an equivalent recognised scheme or standard, such as ISO 27001, then certification under the Cyber Essentials scheme could be waived. Changes to the Cabinet Office Action Note will be tracked by the DfE)
- (Guidance: The department's expectation is that SMEs or organisations of comparable size shall be expected to attain and maintain Cyber Essentials. Larger organisations or enterprises shall be expected to attain and maintain Cyber Essentials Plus.)

12.3. Where clause 12.2 above has not been met, 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, the Department. The scope of certification and the statement of applicability must be acceptable, following review, to the Department, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

– (Guidance: The Department's expectation is that suppliers claiming certification to ISO/IEC 27001 shall provide the Department with copies of their Scope of Certification, Statement of Applicability and a valid ISO/IEC 27001 Certificate issued by an authorised certification body. Where the provider is able to provide a valid Cyber Essentials certification then certification under the ISO/IEC 27001 scheme could be waived and this clause may be removed.)

12.4 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 all 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).

– (Guidance: The Department's expectations are that all contractors shall handle the Department's information in a manner compliant with the GSCP. Details of the GSCP can be found on the GOV.UK website at: https://www.gov.uk/government/publications/government-security-classifications.)

– (Guidance: Compliance with the GCSP removes the requirement for the department to issue a Security Aspects Letter (SAL) to the contractor).

12.5 Departmental Data being handled in the course of providing an ICT solution or service must be separated 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 line with clause 12.14.

– (Guidance: Advice on HMG secure sanitisation policy and approved methods are described at https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)

12.6 The Contractor shall have in place and maintain physical security to premises and sensitive areas in line with ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access), CCTV, alarm systems, etc.

– (Guidance: Where the contractor's and sub-contractor services are wholly carried out within Departmental premises and all access to buildings or ICT systems is managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause.)

12.7 The Contractor shall have in place and maintain an appropriate user access control policy for all ICT systems to ensure only authorised personnel have access to Departmental Data. This policy should include appropriate segregation of duties and if applicable role based access controls (RBAC). User credentials that give access to Departmental Data or systems shall be considered to be sensitive data and must be protected accordingly.

– (Guidance: Where the contractor's and sub-contractor services are wholly carried out within Departmental premises and all access to buildings or ICT systems is managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause.)

12.8 The Contractor shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to:

- physical security controls;
- good industry standard policies and processes;
- malware protection;
- boundary access controls including firewalls, application gateways, etc;
- maintenance and use of fully supported software packages in accordance with vendor recommendations;
- use of secure device configuration and builds;
- software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;
- user identity and access controls, including the use of multi-factor authentication for sensitive data and privileged account accesses;
- any services provided to the department must capture audit logs for security events in an electronic format at the application, service and system level to meet the department's logging and auditing requirements, plus logs shall be:
  - retained and protected from tampering for a minimum period of six months;
  - made available to the department on request.

– (Guidance: Where the contractor's and sub-contractor services are wholly carried out using Departmental ICT resources or locations managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause.)

– (Guidance: The Minimum Cyber Security Standard issued by Cabinet Office and Information Commissioner's Office advice for the protection of sensitive and personal information recommends the use of Multi-Factor Authentication (MFA). The MFA implementation must have two factors as a minimum; with the second factor being facilitated through a separate and discrete channel, such as, a secure web page, voice call, text message or via a purpose built mobile app, such as; Microsoft Authenticator.)

– (Guidance: Further advice on appropriate levels of security audit and log collection to be applied can be found at: https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/c-1-security-monitoring.)

12.9 The contractor shall ensure that any departmental data (including email) transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

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

– (Guidance: The use of an encryption product that utilises the AES256 algorithm would be considered 'industry good practice' in this area. Where the use of removable media as described in this clause is either prohibited or not required in order to deliver the service this clause shall be revised as follows: - 'The use of removable media in any form is not permitted'.)

12.11 The contractor shall ensure that any device which is used to process departmental data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security and https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles.

– (Guidance: The use of an encryption product that utilises the AES256 algorithm would be considered 'industry good practice' in this area. Where the contractor's and sub-contractor services are wholly carried out using Departmental ICT resources managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause.)

12.12 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.

The term 'lock and key' is defined as: "securing information in a lockable desk drawer, cupboard or filing cabinet which is under the user's sole control and to which they hold the keys".

– (Guidance: Further advice on appropriate destruction and disposal methods for physical and hardcopy documents can be found at: https://www.cpni.gov.uk/secure-destruction)

12.13 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.

The term 'under cover' means that the information is carried within an opaque folder or envelope within official premises and buildings and within a closed briefcase or other similar bag or container when outside official premises or buildings.

12.14 In the event of termination of contract due to expiry, liquidation or non-performance, all information assets provided, created or resulting from the service shall not be considered as the supplier's assets and must be returned to the department and written assurance obtained from an appropriate officer of the supplying organisation that these assets regardless of location and format have been fully sanitised throughout the organisation in line with clause 12.15.

- (Guidance: It is Departmental policy that suppliers of business services shall provide evidence of an acceptable level of security assurance concerning sanitisation must be in accordance with guidance provided by NCSC and CPNI.

12.15 In the event of termination, equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored by the Contractor must be accounted for and either physically returned or securely sanitised or destroyed in accordance with the current HMG policy using an NCSC approved product or method.

Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as data stored in a cloud system, Storage Area Network (SAN) or on shared backup tapes, then the Contractor or sub-contractor shall protect the Department's information and data until such time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.

Evidence of secure destruction will be required in all cases.

- (Guidance: Where there is no acceptable secure sanitisation method available for a piece of equipment, or it is not possible to sanitise the equipment due to an irrecoverable technical defect, the storage media involved shall be destroyed using an HMG approved method described at https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media.)
- (Guidance: Further advice on appropriate destruction and disposal methods for physical and hardcopy documents can be found at: https://www.cpni.gov.uk/secure-destruction)
- (Guidance: The term 'accounted for' means that assets and documents retained, disposed of or destroyed should be listed and provided to the department as proof of compliance to this clause.)

12.16 Access by Contractor or sub-contractor staff to Departmental Data, including user credentials, 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. Any Contractor or sub-contractor staff who will be in contact with children or vulnerable adults must, in addition to any security clearance, have successfully undergone an Enhanced DBS (Disclosure and Barring Service) check prior to any contact.

- (Guidance: Further details of the requirements for HMG BPSS clearance are available on the website at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard)
- (Guidance: Further details of the requirements for National Security Vetting, if deemed necessary for this contract are available at: https://www.gov.uk/government/publications/hmg-personnel-security-controls)

12.17 All Contractor or sub-contractor employees who handle Departmental Data shall have annual awareness training in protecting information.

12.18 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.

– (Guidance: The business continuity and disaster recovery plans should be aligned with industry good practice and it is the Department's expectation that all vendors providing services or infrastructure to the Department will have plans that are aligned to the ISO 22301 standard in place. Further information on the requirements of ISO 22301 may be found in the standard.)

12.19 Any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data, including user credentials, used or handled in the course of providing this service shall be recorded as an incident. This includes any non-compliance with these Departmental Security Standards for Contractors, or other Security Standards pertaining to the solution.

Incidents shall be reported to the department immediately, wherever practical, even if unconfirmed or when full details are not known, but always within 24 hours of discovery. If incident reporting has been delayed by more than 24 hours, the contractor should provide an explanation about the delay.

Incidents shall be reported through the department's nominated system or service owner.

Incidents shall be investigated by the contractor with outcomes being notified to the Department.

12.20 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 an NCSC CHECK Scheme 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.

– (Guidance: Further information on IT Health Checks and the NCSC CHECK Scheme which enables penetration testing by NCSC approved companies can be found on the NCSC website at: https://www.ncsc.gov.uk/scheme/penetration-testing.)

12.21 The Contractor or sub-contractors providing the service will provide the Department with full details of any actual or future intent to develop, manage, support, process or store Departmental Data outside of the UK mainland. The Contractor or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Department.

– (Guidance: The offshoring of HMG information outside of the UK is subject to approval by the Departmental SIRO).

12.22 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.

12.23 The Contractor and sub-contractors shall undergo appropriate security assurance activities and shall provide appropriate evidence including the production of the necessary security documentation as determined by the department. 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 Security and Information Risk Advisor (SIRA) certified to NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Cyber Professional (CCP) schemes.

– (Guidance: It is Departmental policy that suppliers of business services shall provide evidence of an acceptable level of security assurance concerning their organisation. Further advice and guidance on the Department's security assurance processes can be supplied on request. Information about the HMG Supplier Assurance Framework can be found at: https://www.gov.uk/government/publications/government-supplier-assurance-framework

– (Guidance: Further information on the CCP and CCSC roles described above can be found on the NCSC website at: https://www.ncsc.gov.uk/information/about-certified-professional-scheme and https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy)

12.24 Where the Contractor is delivering an ICT solution to the Department they shall design and deliver solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current NCSC Information Assurance Guidance and Departmental Policy. The Contractor will provide the Department with evidence of compliance for the solutions and services to be delivered. The Department's expectation is that the Contractor shall provide written evidence of:

- Compliance with HMG Minimum Cyber Security Standard.
- Any existing security assurance for the services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification.
- Any existing HMG security accreditations or assurance that are still valid including: details of the awarding body; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement.
- Documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Contractor shall provide details of who the awarding body or organisation will be and date expected.

12.25 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.

End of Department's Security Standards Clause