	the Secretary of State)	
	anywhere in the world not prohibited by the Buyer	☐
Staff Vetting Procedure (see Paragraph 6)		
The Buyer requires a Staff Vetting Procedure other than BPSS		☐
Where an alternative Staff Vetting Procedure is required, the procedure is: **N/A**		

Optional requirements

1.3 Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements of the corresponding Paragraph. Where the Buyer has not selected an option, the corresponding requirement does not apply.

Security Management Plan (see Paragraph 10)	
The Supplier must provide the Buyer with a Security Management Plan detailing how the requirements for the options selected in this table have been met.	☐
Buyer Security Policies (see Paragraph 11)	
The Buyer requires the Supplier to comply with the following policies relating to security management: • **[List Buyer security policies with which the Supplier and Sub-contractors must comply]**.	☐
Security testing (see Paragraph 12)	
The Supplier must undertake security testing at least once every Contract Year and remediate any vulnerabilities, where it is technically feasible to do so	☒
Cloud Security Principles (see Paragraph 13)	
The Supplier must assess the Supplier System against the Cloud Security Principles	☒
Record keeping (see Paragraph 14)	
The Supplier must keep records relating to Subcontractors, Sites, Third-Party Tools and third parties	☒

Encryption (see Paragraph 15)	
The Supplier must encrypt Government Data while at rest or in transit	☒
Protective Monitoring System (see Paragraph 16)	
The Supplier must implement an effective Protective Monitoring System	☒
Patching (see Paragraph 17)	
The Supplier must patch vulnerabilities in the Supplier System promptly	☒
Malware protection (see Paragraph 18)	
The Supplier must use appropriate Anti-virus Software	☒
End-User Devices (see Paragraph 19)	
The Supplier must manage End-User Devices appropriately	☒
Vulnerability scanning (see Paragraph 20)	
The Supplier must scan the Supplier System monthly for unpatched vulnerabilities	☒
Access control (see Paragraph 21)	
The Supplier must implement effective access control measures for those accessing Government Data and for Privileged Users	☒
Remote Working (see Paragraph 22)	
The Supplier may allow Supplier Staff to undertake Remote Working once an approved Remote Working Policy is in place	☒
Backup and recovery of Government Data (see Paragraph 23)	
The Supplier must have in place systems for the backup and recovery of Government Data	☒
Return and deletion of Government Data (see Paragraph 24)	
The Supplier must return or delete Government Data when requested by the Buyer	☒
Physical security (see Paragraph 25)	
The Supplier must store Government Data in physically secure locations	☒
Security breaches (see Paragraph 26)	

The Supplier must report any Breach of Security to the Buyer promptly	☒

2 DEFINITIONS

"Anti-virus Software" means software that:

a. protects the Supplier System from the possible introduction of Malicious Software;

b. scans for and identifies possible Malicious Software in the Supplier System;

c. if Malicious Software is detected in the Supplier System, so far as possible:

i. prevents the harmful effects of the Malicious Software; and

ii. removes the Malicious Software from the Supplier System;

"BPSS" means the employment controls applied to any individual member of the Supplier Staff that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 7.0, June 2024 (https://www.gov.uk/government/publications/government-baseline-personnel-security-standard), as that document is updated from time to time;

"Breach of Security" means the occurrence of:

a. any unauthorised access to or use of the Services, the Sites, the Supplier System and/or the Government Data;

b. the loss (physical or otherwise), corruption and/or unauthorised disclosure of any Government Data, including copies of such Government Data; and/or

c. any part of the Supplier System ceasing to be compliant with the required Certifications;

d. the installation of Malicious Software in the Supplier System:

e. any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the Supplier System; and

f. includes any attempt to undertake the activities listed in sub-Paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:

i. was part of a wider effort to access information and communications technology operated by or on behalf of

Central Government Bodies; or

ii. was undertaken, or directed by, a state other than the United Kingdom;

"Buyer Equipment" means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System;

"Buyer Security Policies" means those securities specified by the Buyer in Paragraph 1.3;

"Buyer System" means the Buyer's information and communications technology system, including any software or Buyer Equipment, owned by the Buyer or leased or licenced to it by a third-party, that:

a. is used by the Buyer or Supplier in connection with this Contract;

b. interfaces with the Supplier System; and/or

c. is necessary for the Buyer to receive the Services.

"Certifications" means one or more of the following certifications (or equivalent):

a. ISO/IEC 27001:2022 by a UKAS- recognised Certification Body in respect of the Supplier System, or in respect of a wider system of which the Supplier System forms part; and

b. Cyber Essentials Plus; and/or

c. Cyber Essentials;

"CHECK Scheme" means the NCSC's scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks;

"CHECK Service Provider" means a company which, under the CHECK Scheme:

a. has been certified by the NCSC;

b. holds "Green Light" status; and

c. is authorised to provide the IT Health Check services required by Paragraph 9.2 (*Security Testing*);

"Cloud Security Principles" means the NCSC's document "Implementing the Cloud Security Principles" as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles;

"Contract Year" means:

1. a period of 12 months commencing on the Start Date;

2. thereafter a period of 12 months commencing on each anniversary of

	the Start Date; a. with the final Contract Year ending on the expiry or termination of the Term;
"CREST Service Provider"	means a company with an information security accreditation of a security operations centre qualification from CREST International;
"Cyber Essentials"	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Plus"	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Scheme"	means the Cyber Essentials scheme operated by the NCSC;
"Developed System"	means the software or system that the Supplier is required to develop under this Contract;
"End-User Device"	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic devices used in the provision of the Services;
"Expected Behaviours"	means the expected behaviours set out and updated from time to time in the Government Security Classification Policy, currently found at paragraphs 12 to 16 and in the table below paragraph 16 of https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html;
"Government Data"	Means any: . a. data, texts, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media; b. Personal Data for which the Buyer is a, or the, Data Controller; or c. any meta-data relating to categories of data referred to in Paragraphs (a) or (b); that is: d. supplied to the Supplier by or on behalf of the Buyer; or e. that the Supplier is required to generate, Process, Handle, store or transmit under this Contract;
"Government Security Classification	means the policy, as updated from time to time, establishing an administrative system to protect information assets appropriately against prevalent threats, including classification tiers, protective security controls and baseline behaviours, the current version of which is found at https://www.gov.uk/

Policy"	government/publications/government-security-classifications;
"Handle"	means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data;
"IT Health Check"	means the security testing of the Supplier System;
"Malicious Software"	means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations;
"NCSC"	means the National Cyber Security Centre, or any successor body performing the functions of the National Cyber Security Centre;
"NCSC Device Guidance"	means the NCSC's document "Device Security Guidance", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance;
"Privileged User"	means a user with system administration access to the Supplier System, or substantially similar access privileges;
"Prohibition Notice"	means the meaning given to that term by Paragraph 4.4.
"Protective Monitoring System"	has the meaning given to that term by Paragraph 13.1;
"Relevant Conviction"	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences) or any other offences relevant to Services as the Buyer may specify;
"Remote Location"	means [the relevant Supplier Staff's permanent home address authorised by the Supplier or Sub-contractor (as applicable) for Remote Working OR a location other than a Supplier's or a Sub-contractor's Site];
"Remote Working"	means the provision or management of the Services by Supplier Staff from a location other than a Supplier's or a Sub-contractor's Site;
"Remote Working Policy"	the policy prepared and approved under Paragraph 22 under which Supplier Staff are permitted to undertake Remote Working;
"Security Controls"	means the security controls set out and updated from time to time in the Government Security Classification Policy, currently found at Paragraph 12 of https://www.gov.uk/government/publications/government-security-

classifications/guidance-15-considerations-for-security-advisors-html;

"Sites" means any premises (including the Buyer's Premises, the Supplier's premises or third party premises):

a. from, to or at which:

i. the Services are (or are to be) provided; or

ii. the Supplier manages, organises or otherwise directs the provision or the use of the Services; or

b. where:

i. any part of the Supplier System is situated; or

ii. any physical interface with the Buyer System takes place;

"Staff Vetting Procedure" means the procedure for vetting Supplier Staff set out in Paragraph 6;

"Subcontractor Staff" means:

a. any individual engaged, directly or indirectly, or employed, by any Subcontractor; and

b. engaged in or likely to be engaged in:

i. the performance or management of the Services; or

ii. the provision of facilities or services that are necessary for the provision of the Services;

Supplier System" means

a. any:

i. information assets,

ii. IT systems,

iii. IT services; or

iv. Sites,

that the Supplier or any Subcontractor will use to Handle, or support the Handling of, Government Data and provide, or support the provision of, the Services; and

b. the associated information management system, including all relevant:

i. organisational structure diagrams;

ii. controls;

iii. policies;

iv. practices;

v. procedures;

vi. processes; and

vii. resources;

"Third-party Tool"	means any software used by the Supplier by which the Government Data is accessed, analysed or modified, or some form of operation is performed on it;
"UKAS-recognised Certification Body"	means: a. an organisation accredited by UKAS to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022; or b. an organisation accredited to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022 by a body with the equivalent functions as UKAS in a state with which the UK has a mutual recognition agreement recognising the technical equivalence of accredited conformity assessment.

PART ONE: CORE REQUIREMENTS

3 HANDLING GOVERNMENT DATA

3.1 The Supplier acknowledges that it:

3.1.1 must only Handle Government Data that is classified as OFFICIAL; and

3.1.2 must not Handle Government Data that is classified as SECRET or TOP SECRET.

3.2 The Supplier must:

3.2.1 not alter the classification of any Government Data.

3.2.2 if it becomes aware that it has Handled any Government Data classified as SECRET or TOP SECRET the Supplier must:

i. immediately inform the Buyer; and

ii. follow any instructions from the Buyer concerning the Government Data.

3.3 The Supplier must, and must ensure that Sub-contractors and Supplier Staff, when Handling Government Data, comply with:

3.3.1 the Expected Behaviours; and

3.3.2 the Security Controls.

4 CERTIFICATION REQUIREMENTS

4.1 Where the Buyer has not specified Certifications under Paragraph 1, the Supplier must ensure that it and any Subcontractors that Handle Government Data are certified as compliant with Cyber Essentials (or equivalent).

4.2 Where the Buyer has specified Certifications under Paragraph 1, the Supplier must ensure that both:

4.2.1 it; and

4.2.2 any Subcontractor that Processes Government Data, are certified as compliant with the Certifications specified by the Buyer in Paragraph 1 (or equivalent certifications):

4.3 The Supplier must ensure that the specified Certifications (or their equivalent) are in place for it and any relevant Subcontractor:

4.3.1 before the Supplier or any Subcontractor Handles Government Data; and

4.3.2 throughout the Term.

5 LOCATION

5.1 Where the Buyer has not specified any locations or territories in Paragraph 1, the Supplier must not, and ensure that Subcontractors do not store, access or Handle Government Data outside:

5.1.1 the United Kingdom; or

5.1.2 a location permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).

5.2 Where the Buyer has specified locations or territories in Paragraph 1, the Supplier must, and ensure that all Subcontractors, at all times store, access or Handle Government Data only in or from the geographic areas specified by the Buyer.

5.3 The Supplier must, and must ensure that its Subcontractors store, access or Handle Government Data in a facility operated by an entity where:

5.3.1 the entity has entered into a binding agreement with the Supplier or Subcontractor (as applicable);(b) that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Subcontractors in this Annex;

5.3.2 the Supplier or Subcontractor has taken reasonable steps to assure itself that:

i. the entity complies with the binding agreement; and

ii. the Subcontractor's system has in place appropriate technical and organisational measures to ensure that the Subcontractor will store, access, manage and/or Process the Government Data as required by this Annex;

5.3.3 the Buyer has not given the Supplier a Prohibition Notice under Paragraph 4.4.

5.4 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Subcontractors must not undertake or permit to be undertaken the storage, accessing or Processing of Government Data in one or more countries or territories (a "**Prohibition Notice**").

5.5 Where the Supplier must and must ensure Subcontractors comply with the requirements of a Prohibition Notice within 40 Working Days of the date of the notice.

6 STAFF VETTING

6.1 The Supplier must not allow Supplier Staff, and must ensure that Subcontractors do not allow Subcontractor Staff, to access or Handle Government Data, if that person:

6.1.1 has not completed the Staff Vetting Procedure; or

6.1.2 where no Staff Vetting Procedure is specified in the Order Form:

i. has not undergone the checks required for the BPSS to verify:

A. the individual's identity;

B. where that individual will work in the United Kingdom, the individual's nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom; and

C. the individual's previous employment history; and

D. that the individual has no Relevant Convictions; and

ii. national security vetting clearance to the level specified by the Authority for such individuals or such roles as the Authority may specify.

6.2 Where the Supplier considers it cannot ensure that a Sub-contractor will undertake the relevant security checks on any Sub-contractor Staff, it must:

6.2.1 as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;

6.2.2 provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Sub-contractor staff will perform as the Buyer reasonably requires; and

6.2.3 comply, at the Supplier's cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Staff and the management of the Sub-contract.

7 SUPPLIER ASSURANCE LETTER

7.1 The Supplier must, no later than the last day of each Contract Year, provide to the Buyer a letter from its chief technology officer (or equivalent officer) confirming that, having made due and careful enquiry:

7.1.1 the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters required by this Contract;

7.1.2 it has fully complied with all requirements of this Annex; and

7.1.3 all Subcontractors have complied with the requirements of this Annex with which the Supplier is required to ensure they comply;

7.1.4 the Supplier considers that its security and risk mitigation procedures remain effective.

8 ASSURANCE

8.1 The Supplier must provide such information and documents as the Buyer may request in order to demonstrate the Supplier's and any Subcontractors' compliance with this Annex.

8.2 The Supplier must provide that information and those documents:

8.2.1 at no cost to the Buyer;

8.2.2 within 10 Working Days of a request by the Buyer;

8.2.3 except in the case of original document, in the format and with the content and information required by the Buyer; and

8.2.4 in the case of original document, as a full, unedited and unredacted copy.

9 USE OF SUBCONTRACTORS AND THIRD PARTIES

9.1 The Supplier must ensure that Subcontractors and any other third parties that store, have access to or Handle Government Data comply with the requirements of this Annex.

PART TWO: ADDITIONAL REQUIREMENTS

10 SECURITY MANAGEMENT PLAN

10.1 This Paragraph 10 applies only where the Buyer has selected this option in Paragraph 1.3.

Preparation of Security Management Plan

10.2 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Annex and the Contract in order to ensure the security of the Supplier solution and the Buyer data.

10.3 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Contract, the Security Management Plan, which must include a description of how all the options selected in this Annex are being met along with evidence of the required certifications for the Supplier and any Subcontractors specified in Paragraph 3. iThe Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and must issue the Supplier with either:

10.3.1 an information security approval statement, which shall confirm that the Supplier may operate the service and process Buyer data; or

10.3.2 a rejection notice, which shall set out the Buyer's reasons for rejection the Security Management Plan.

10.4 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within 10 Working Days of the date of the rejection, or such other period agreed with the Buyer.

10.5 The process set out in Paragraph 10.5 shall be repeated until such time as the Authority issues a Risk Management Approval Statement to the Supplier or terminates this Contract.

10.6 The rejection by the Buyer of a second revised Security Management Plan is a material Default of this Contract.

Updating Security Management Plan

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

Monitoring

10.8 The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:

10.8.1 a significant change to the components or architecture of the Supplier System;

10.8.2 a new risk to the components or architecture of the Supplier System;

10.8.3 a vulnerability to the components or architecture of the Supplier System using an industry standard vulnerability scoring mechanism;

10.8.4 a change in the threat profile;

10.8.5 a significant change to any risk component;

10.8.6 a significant change in the quantity of Personal Data held within the Service;

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

10.8.8 an ISO27001 audit report produced in connection with the Certification indicates significant concerns.

10.9 Within 10 Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Security Management Plan and submit the updated Security Management Plan to the Buyer for review and approval.

11 BUYER SECURITY POLICIES

11.1 The Supplier must comply, when it provides the Services and operates and manages the Supplier System, with all Buyer Security Policies identified in the relevant option in Paragraph 1.3.

11.2 If there is an inconsistency between the Buyer Security Policies and the requirement of this Annex, then the requirements of this Annex will prevail to the extent of that inconsistency.

12 SECURITY TESTING

12.1 The Supplier must:

12.1.1 before Handling Government Data;

12.1.2 at least once during each Contract Year; and undertake the following activities:

12.1.3 conduct security testing of the Supplier System (an "**IT Health Check**") in accordance with Paragraph 12.2; and

12.1.4 implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph 12.3.

12.2 In arranging an IT Health Check, the Supplier must:

12.2.1 use only a CHECK Service Provider or CREST Service Provider to perform the IT Health Check;

12.2.2 design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier System and the delivery of the Services;

12.2.3 ensure that the scope of the IT Health Check encompasses the components of the Supplier System used to access, store, Process or manage Government Data; and

12.2.4 ensure that the IT Health Check provides for effective penetration testing of the Supplier System.

12.3 The Supplier treat any vulnerabilities as follows:

12.3.1 the Supplier must remedy any vulnerabilities classified as high in the IT Health Check report:

i. if it is technically feasible to do so, within 5 Working Days of becoming aware of the vulnerability and its classification; or

ii. if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3(a)(i) , then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

12.3.2 the Supplier must remedy any vulnerabilities classified as high in the IT Health Check report:

i. if it is technically feasible to do so, within 1 month of becoming aware of the vulnerability and its classification; or

ii. if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3(b)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

12.3.3 the Supplier must remedy any vulnerabilities classified as medium in the IT Heath Check report:

i. if it is technically feasible to do so, within 3 months of becoming aware of the vulnerability and its classification; or

ii. if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3(c)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

12.3.4 where it is not technically feasible to remedy the vulnerability, the Supplier must implement appropriate technical and organisational measures to mitigate the risk posed by the vulnerability.

13 CLOUD SECURITY PRINCIPLES

13.1 The Supplier must ensure that the Supplier System complies with the Cloud Security Principles.

13.2 The Supplier must assess the Supplier System against the Cloud Security Principles to assure itself that it complies with Paragraph 10.1:

13.2.1 before Handling Government Data;

13.2.2 at least once each Contract Year; and

13.2.3 when required by the Buyer.

13.3 Where the Cloud Security Principles provide for various options, the Supplier must document the option it has chosen to implement and its reasons for doing do.

13.4 The Supplier must:

13.4.1 keep records of any assessment that it makes under Paragraph 13.2; and

13.4.2 provide copies of those records to the Buyer within 10 Working Days of any request by the Buyer.

14 INFORMATION ABOUT SUBCONTRACTORS, SITES AND THIRD-PARTY TOOLS

14.1 The Supplier must keep the following records:

14.1.1 for Subcontractors or third parties that store, have access to or Handle Government Data:

i. the Subcontractor or third party's name:

A. legal name;

B. trading name (if any); and

C. registration details (where the Subcontractor is not an individual), including:

a) country of registration;

b) registration number (if applicable); and

c) registered address;

D. the Certifications held by the Subcontractor or third party;

E. the Sites used by the Subcontractor or third party;

F. the Services provided or activities undertaken by the Subcontractor or third party;

G. the access the Subcontractor or third party has to the Supplier System;

H. the Government Data Handled by the Subcontractor or third party; and

I. the measures the Subcontractor or third party has in place to comply with the requirements of this Annex;

ii. for Sites from or at which Government Data is accessed or Handled:

A. the location of the Site;

B. the operator of the Site, including the operator's:

a) legal name;

b) trading name (if any); and

c) registration details (where the Subcontractor is not an individual);

d) the Certifications that apply to the Site;

e) the Government Data stored at, or Handled from, the site; and

iii. for Third-party Tools:

A. the name of the Third-Party Tool;

iv. the nature of the activity or operation performed by the Third-Party Tool on the Government Data; and

A. in respect of the entity providing the Third-Party Tool, its:

B. full legal name;

C. trading name (if any)

D. country of registration;

E. registration number (if applicable); and

F. registered address.

14.2 The Supplier must update the records it keeps in accordance with Paragraph 14.1:

14.2.1 at least four times each Contract Year;

14.2.2 whenever a Subcontractor, third party that accesses or Handles Government Data, Third-party Tool or Site changes; or

14.2.3 whenever required to go so by the Buyer.

14.3 The Supplier must provide copies of the records it keeps in accordance with Paragraph 14.1 to the Buyer within 10 Working Days of any request by the Buyer.

15 ENCRYPTION

15.1 The Supplier must, and must ensure that all Subcontractors, encrypt Government Data:

15.1.1 when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and

15.1.2 when transmitted.

16 PROTECTIVE MONITORING SYSTEM

16.1 The Supplier must, and must ensure that Subcontractors, implement an effective system of monitoring and reports, analysing access to and use of the Supplier System and the Government Data to:

16.1.1 identify and prevent any potential Breach of Security;

16.1.2 respond effectively and in a timely manner to any Breach of Security that does;

16.1.3 identify and implement changes to the Supplier System to prevent future any Breach of Security; and

16.1.4 help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier System, (the "**Protective Monitoring System**").

16.2 The Protective Monitoring System must provide for:

16.2.1 event logs and audit records of access to the Supplier System; and

16.2.2 regular reports and alerts to identify:

i. changing access trends;

ii. unusual usage patterns; or

iii. the access of greater than usual volumes of Government Data; and

iv. the detection and prevention of any attack on the Supplier System using common cyber-attack techniques.

17 PATCHING

17.1 The Supplier must, and must ensure that Subcontractors, treat any public releases of patches for vulnerabilities as follows:

17.1.1 the Supplier must patch any vulnerabilities classified as "**critical**":

i. if it is technically feasible to do so, within 5 Working Days of the public release; or

ii. if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 17.1(a)(i), then as soon as reasonably practicable after the public release;

17.1.2 the Supplier must patch any vulnerabilities classified as "**important**":

i. if it is technically feasible to do so, within 1 month of the public release; or

ii. if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 17.1(b)(i), then as soon as reasonably practicable after the public release;

17.1.3 the Supplier must remedy any vulnerabilities classified as "**other**" in the public release:

i. if it is technically feasible to do so, within 2 months of the public release; or

ii. if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 17.1(c)(i), then as soon as reasonably practicable after the public release;

17.1.4 where it is not technically feasible to patch the vulnerability, the Supplier must implement appropriate technical and organisational measures to mitigate the risk posed by the vulnerability.

18 MALWARE PROTECTION

18.1 The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier System.

18.2 The Supplier must ensure that such Anti-virus Software:

18.2.1 prevents the installation of the most common forms of Malicious Software in the Supplier System;

18.2.2 performs regular scans of the Supplier System to check for Malicious Software; and

18.2.3 where Malicious Software has been introduced into the Supplier System, so far as practicable

i. prevents the harmful effects from the Malicious Software; and

ii. removes the Malicious Software from the Supplier System.

19 END-USER DEVICES

19.1 The Supplier must, and must ensure that all Subcontractors, manage all End-User Devices on which Government Data is stored or Handled in accordance with the following requirements:

19.1.1 the operating system and any applications that store, Handle or have access to Government Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;

19.1.2 users must authenticate before gaining access;

19.1.3 all Government Data must be encrypted using a suitable encryption tool;

19.1.4 the End-User Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-User Device is inactive;

19.1.5 the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Government Data to ensure the security of that Government Data;

19.1.6 the Supplier or Subcontractor, as applicable, can, without physical access to the End-User Device, remove or make inaccessible all Government Data stored on the device and prevent any user or group of users from accessing the device;

19.1.7 all End-User Devices are within the scope of any required Certification.

19.2 The Supplier must comply, and ensure that all Subcontractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Contract.

20 VULNERABILITY SCANNING

20.1 The Supplier must:

20.1.1 scan the Supplier System at least once every month to identify any unpatched vulnerabilities; and

20.1.2 if the scan identifies any unpatched vulnerabilities, ensure they are patched in accordance with Paragraph 14.

21 ACCESS CONTROL

21.1 The Supplier must, and must ensure that all Subcontractors:

21.1.1 identify and authenticate all persons who access the Supplier System before they do so;

21.1.2 require multi-factor authentication for all user accounts that have access to Government Data or that are Privileged Users;

21.1.3 allow access only to those parts of the Supplier System and Sites that those persons require;

21.1.4 maintain records detailing each person's access to the Supplier System.

21.2 The Supplier must ensure, and must ensure that all Subcontractors ensure, that the user accounts for Privileged Users of the Supplier System:

21.2.1 are allocated to a single, individual user;

21.2.2 are accessible only from dedicated End-User Devices;

21.2.3 are configured so that those accounts can only be used for system administration tasks;

21.2.4 require passwords with high complexity that are changed regularly;

21.2.5 automatically log the user out of the Supplier System after a period of time that is proportionate to the risk environment during which the account is inactive; and

21.2.6 are:

i. restricted to a single role or small number of roles;

ii. time limited; and

iii. restrict the Privileged User's access to the internet.

22 REMOTE WORKING

22.1 The Supplier must ensure, and ensure that Sub-contractors ensure, that:

22.1.1 unless in writing by the Authority, Privileged Users do not undertake Remote Working;

22.1.2 where the Authority permits Remote Working by Privileged Users, the Supplier ensures, and ensures that Sub-contractors ensure, that such Remote Working takes place only in accordance with any conditions imposed by the Authority.

22.2 Where the Supplier or a Sub-contractor wishes to permit Supplier Staff to undertake Remote Working, it must:

22.2.1 prepare and have approved by the Buyer in the Remote Working Policy in accordance with this Paragraph;

22.2.2 undertake and, where applicable, ensure that any relevant Sub-contractors undertake, all steps required by the Remote Working Policy;

22.2.3 ensure that Supplier Staff undertake Remote Working only in accordance with the Remote Working Policy;

22.2.4 may not permit any Supplier Staff or the Supplier or any Sub-contractor to undertake Remote Working until the Remote Working Policy is approved by the Buyer.

22.3 The Remote Working Policy must include or make provision for the following matters:

22.3.1 restricting or prohibiting Supplier Staff from printing documents in any Remote Location;

22.3.2 restricting or prohibiting Supplier Staff from downloading any Government Data to any End-User Device other than an End User Device that:

i. is provided by the Supplier or Sub-contractor (as appropriate); and

ii. complies with the requirements set out in Paragraph 3 (*End-User Devices*);

22.3.3 ensuring that Supplier Staff comply with the Expected Behaviours (so far as they are applicable);

22.3.4 giving effect to the Security Controls (so far as they are applicable); and

22.3.5 for each different category of Supplier Staff subject to the proposed Remote Working Policy:

i. the types and volumes of Government Data that the Supplier Staff can Handle in a Remote Location and the Handling that those Supplier Staff will undertake;

ii. any identified security risks arising from the proposed Handling in a Remote Location;

iii. the mitigations, controls and security measures the Supplier or Sub-contractor (as applicable) will implement to mitigate the identified risks; and

iv. the business rules with which the Supplier Staff must comply.

22.4 The Supplier may submit a proposed Remote Working Policy for consideration at any time.

23 BACKUP AND RECOVERY OF GOVERNMENT DATA

23.1 The Supplier must ensure that the Supplier System:

23.1.1 backs up and allows for the recovery of Government Data to achieve the recovery point and recovery time objectives specified by the Buyer, or in accordance with Good Industry Practice where the Buyer has not specified; and

23.1.2 retains backups of the Government Data for the period specified by the Buyer, or in accordance with Good Industry Practice where the Buyer has not specified.

23.2 The Supplier must ensure the Supplier System:

23.2.1 uses backup location for Government Data that are physically and logically separate from the rest of the Supplier System;

23.2.2 the backup system monitors backups of Government Data to:

i. identify any backup failure; and

ii. confirm the integrity of the Government Data backed up;

23.2.3 any backup failure is remedied properly;

23.2.4 the backup system monitors backups of Government Data to:

i. identify any recovery failure; and

ii. confirm the integrity of Government Data recovered; and

23.2.5 any recovery failure is promptly remedied.

24 RETURN AND DELETION OF GOVERNMENT DATA

24.1 Subject to Paragraph 24.2, when requested to do so by the Buyer, the Supplier must, and must ensure that all Subcontractors:

24.1.1 securely erase any or all Government Data held by the Supplier or Subcontractor using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted; or

24.1.2 provide the Buyer with copies of any or all Government Data held by the Supplier or Subcontractor using the method specified by the Buyer.

24.2 Paragraph 24.1 does not apply to Government Data:

24.2.1 that is Personal Data in respect of which the Supplier is a Controller;

24.2.2 to which the Supplier has rights to Handle independently from this Contract; or

24.2.3 in respect of which, the Supplier is under an obligation imposed by Law to retain.

24.3 The Supplier must, and must ensure that all Sub-contractors, provide the Buyer with copies of any or all Buyer Data held by the Supplier or Sub-contractor:

24.3.1 when requested to do so by the Buyer; and

24.3.2 using the method specified by the Buyer.

25 PHYSICAL SECURITY

25.1 The Supplier must, and must ensure that Subcontractors, store the Government Data on servers housed in physically secure locations.

26 BREACH OF SECURITY

26.1 If the Supplier becomes aware of a Breach of Security that impacts or has the potential to impact the Government Data, it shall:

26.1.1 notify the Buyer as soon as reasonably practicable after becoming aware of the breach, and in any event within [24] hours;

26.1.2 provide such assistance to the Buyer as the Buyer requires until the Breach of Security and any impacts or potential impacts on the Buyer are resolved to the Buyer's satisfaction;

26.1.3 where the Law requires the Buyer to report a Breach of Security to the appropriate regulator provide such information and other input as the Buyer requires within the timescales specified by the Buyer.

SCHEDULE 9: INVOICING REQUIREMENTS

In this Schedule 9:

- References to "Buyer" shall mean the Employer
- References to "Supplier" shall mean the Contractor
- Unless the context otherwise requires, defined terms shall, save where they are defined in this Schedule 8, have the meanings ascribed to them in this Contract

1. INVOICING

1.1. Invoices shall be submitted electronically by e-mail directly to:

DfE Capital – Accounts.PAYABLE@education.gov.uk

within 30 days of the end of the relevant invoicing date. Other contacts requiring sight of the invoice can be copied in.

1.2. An invoice is only valid if it is legible and includes:

1.2.1. the date of the invoice

1.2.2. Supplier's full name and address

1.2.3. Full valid purchase order number, including the pre-fix:

CAPITAL D-PO-

1.2.4. the charging period

1.2.5. a detailed line level breakdown of the appropriate Charges including Deliverables provided or Milestones Achieved (if applicable)

1.2.6. days and times worked (if applicable)

1.2.7. Service Credits (if applicable)

1.2.8. VAT (if applicable)

1.3. Invoices without a valid purchase order are now rejected by the Buyers e-invoicing solution. The Buyer no longer accepts paper invoices.

SCHEDULE 10: DEED OF GUARANTEE

DATED 20[ ]

[GUARANTOR]

DEED OF GUARANTEE

relating to the provision of
Minor Works for the Older Buildings Research Project for Southern England

THIS DEED OF GUARANTEE is made the ** day of June 2025

PROVIDED BY:

[ ], a company incorporated in England and Wales, with number **[ ]** whose registered office is at **[ ]** (**"Guarantor"**)

WHEREAS:

(A) The Guarantor has agreed, in consideration of the Beneficiary entering into the Guaranteed Agreement with the Supplier, to guarantee all of the Supplier's obligations under the Guaranteed Agreement.

(B) It is the intention of the Parties that this document be executed and take effect as a deed.

Now in consideration of the Beneficiary entering into the Guaranteed Agreement, the Guarantor hereby agrees for the benefit of the Beneficiary as follows:

1. DEFINITIONS AND INTERPRETATION

In this Deed of Guarantee:

1.1 unless defined elsewhere in this Deed of Guarantee or the context requires otherwise, defined terms shall have the same meaning as they have for the purposes of the Guaranteed Agreement;

1.2 the words and phrases below shall have the following meanings:

"Beneficiary"	**THE SECRETARY OF STATE FOR EDUCATION** of Sanctuary Buildings, Great Smith Street, London, SW1P 3BT
"Guaranteed Agreement"	means the contract with Contract Reference [ ] for the provision of minor works to support the older buildings research project (incorporating the conditions of the JCT Measured Term Contract 2016 Edition) for the Works dated on or about the date hereof made between the Beneficiary and the Supplier;
"Guaranteed Obligations"	means all obligations and liabilities of the Supplier to the Beneficiary under the Guaranteed Agreement together with all obligations owed by the Supplier to the Beneficiary that are supplemental to, incurred under, ancillary to or calculated by reference to the Guaranteed Agreement;

"Works"	has the meaning given to it in this Contract;
"Supplier"	means **ETEC CONTRACT SERVICES LIMITED**, whose registered office address is **7, Elmhurst, 98-106 High Rd, London E18 2QH**, with the company house number 05392794.

1.3 references to this Deed of Guarantee and any provisions of this Deed of Guarantee or to any other document or agreement (including to the Guaranteed Agreement) are to be construed as references to this Deed of Guarantee, those provisions or that document or agreement in force for the time being and as amended, varied, restated, supplemented, substituted or novated from time to time;

1.4 unless the context otherwise requires, words importing the singular are to include the plural and vice versa;

1.5 references to a person are to be construed to include that person's assignees or transferees or successors in title, whether direct or indirect;

1.6 the words "other" and "otherwise" are not to be construed as confining the meaning of any following words to the class of thing previously stated where a wider construction is possible;

1.7 unless the context otherwise requires, reference to a gender includes the other gender and the neuter;

1.8 unless the context otherwise requires, references to an Act of Parliament, statutory provision or statutory instrument include a reference to that Act of Parliament, statutory provision or statutory instrument as amended, extended or re-enacted from time to time and to any regulations made under it;

1.9 unless the context otherwise requires, any phrase introduced by the words "including", "includes", "in particular", "for example" or similar, shall be construed as illustrative and without limitation to the generality of the related general words;

1.10 references to Clauses and Schedules are, unless otherwise provided, references to Clauses and Schedules to this Deed of Guarantee; and

1.11 references to liability are to include any liability whether actual, contingent, present or future.

2. GUARANTEE AND INDEMNITY

2.1 The Guarantor irrevocably and unconditionally guarantees and undertakes to the Beneficiary to procure that the Supplier duly and punctually performs all of the Guaranteed Obligations now or hereafter due, owing or incurred by the Supplier to the Beneficiary.

2.2 The Guarantor irrevocably and unconditionally undertakes upon demand to pay to the Beneficiary all monies and liabilities which are now or at any time hereafter shall have become payable by the Supplier to the Beneficiary

under or in connection with the Guaranteed Agreement or in respect of the Guaranteed Obligations as if it were a primary obligor.

2.3 If at any time the Supplier shall fail to perform any of the Guaranteed Obligations, the Guarantor, as primary obligor, irrevocably and unconditionally undertakes to the Beneficiary that, upon first demand by the Beneficiary it shall, at the cost and expense of the Guarantor:

2.3.1 fully, punctually and specifically perform such Guaranteed Obligations as if it were itself a direct and primary obligor to the Beneficiary in respect of the Guaranteed Obligations and liable as if the Guaranteed Agreement had been entered into directly by the Guarantor and the Beneficiary; and

2.3.2 as a separate and independent obligation and liability, indemnify and keep the Beneficiary indemnified against all losses, damages, costs and expenses (including VAT thereon, and including all court costs and all legal fees on a solicitor and own client basis, together with any disbursements,) of whatever nature which may result or which such Beneficiary may suffer, incur or sustain arising in any way whatsoever out of a failure by the Supplier to perform the Guaranteed Obligations save that, subject to the other provisions of this Deed of Guarantee, this shall not be construed as imposing greater obligations or liabilities on the Guarantor than are purported to be imposed on the Supplier under the Guaranteed Agreement.

2.4 As a separate and independent obligation and liability from its obligations and liabilities under Clauses 2.1 to 2.3 above, the Guarantor as a primary obligor irrevocably and unconditionally undertakes to indemnify and keep the Beneficiary indemnified on demand against all losses, damages, costs and expenses (including VAT thereon, and including all legal costs and expenses), of whatever nature, whether arising under statute, contract or at common law, which such Beneficiary may suffer or incur if any obligation guaranteed by the Guarantor is or becomes unenforceable, invalid or illegal as if the obligation guaranteed had not become unenforceable, invalid or illegal provided that the Guarantor's liability shall be no greater than the Supplier's liability would have been if the obligation guaranteed had not become unenforceable, invalid or illegal.

3. OBLIGATION TO ENTER INTO A NEW CONTRACT

If the Guaranteed Agreement is terminated for any reason, whether by the Beneficiary or the Supplier, or if the Guaranteed Agreement is disclaimed by a liquidator of the Supplier or the obligations of the Supplier are declared to be void or voidable for any reason, then the Guarantor will, at the request of the Beneficiary enter into a contract with the Beneficiary in terms mutatis mutandis the same as the Guaranteed Agreement and the obligations of the Guarantor under such substitute agreement shall be the same as if the Guarantor had been original obligor under the Guaranteed Agreement or under an agreement entered into on the same terms and at the same time as the Guaranteed Agreement with the Beneficiary.

4. DEMANDS AND NOTICES

4.1 Any demand or notice served by the Beneficiary on the Guarantor under this Deed of Guarantee shall be in writing, addressed to:

3rd Floor 86 - 90 Paul Street, London, England, EC2A 4NE

For the Attention [redacted]

or such other address in England and Wales or facsimile number as the Guarantor has from time to time notified to the Beneficiary in writing in accordance with the terms of this Deed of Guarantee as being an address or facsimile number for the receipt of such demands or notices.

4.2 Any notice or demand served on the Guarantor or the Beneficiary under this Deed of Guarantee shall be deemed to have been served:

4.2.1 if delivered by hand, at the time of delivery; or

4.2.2 if posted, at 10.00 a.m. on the second Working Day after it was put into the post; or

4.2.3 if sent by facsimile, at the time of despatch, if despatched before 5.00 p.m. on any Working Day, and in any other case at 10.00 a.m. on the next Working Day.

4.3 In proving service of a notice or demand on the Guarantor or the Beneficiary it shall be sufficient to prove that delivery was made, or that the envelope containing the notice or demand was properly addressed and posted as a prepaid first class recorded delivery letter, or that the facsimile message was properly addressed and despatched, as the case may be.

4.4 Any notice purported to be served on the Beneficiary under this Deed of Guarantee shall only be valid when received in writing by the Beneficiary.

5. BENEFICIARY'S PROTECTIONS

5.1 The Guarantor shall not be discharged or released from this Deed of Guarantee by any arrangement made between the Supplier and the Beneficiary (whether or not such arrangement is made with or without the assent of the Guarantor) or by any amendment to or termination of the Guaranteed Agreement or by any forbearance or indulgence whether as to payment, time, performance or otherwise granted by the Beneficiary in relation thereto (whether or not such amendment, termination, forbearance or indulgence is made with or without the assent of the Guarantor) or by the Beneficiary doing (or omitting to do) any other matter or thing which but for this provision might exonerate the Guarantor.

5.2 This Deed of Guarantee shall be a continuing security for the Guaranteed Obligations and accordingly:

5.2.1 it shall not be discharged, reduced or otherwise affected by any partial performance (except to the extent of such partial performance) by the Supplier of the Guaranteed Obligations or by

any omission or delay on the part of the Beneficiary in exercising its rights under this Deed of Guarantee;

5.2.2 it shall not be affected by any dissolution, amalgamation, reconstruction, reorganisation, change in status, function, control or ownership, insolvency, liquidation, administration, appointment of a receiver, voluntary arrangement, any legal limitation or other incapacity, of the Supplier, the Beneficiary, the Guarantor or any other person;

5.2.3 if, for any reason, any of the Guaranteed Obligations shall prove to have been or shall become void or unenforceable against the Supplier for any reason whatsoever, the Guarantor shall nevertheless be liable in respect of that purported obligation or liability as if the same were fully valid and enforceable and the Guarantor were principal debtor in respect thereof; and

5.2.4 the rights of the Beneficiary against the Guarantor under this Deed of Guarantee are in addition to, shall not be affected by and shall not prejudice, any other security, guarantee, indemnity or other rights or remedies available to the Beneficiary.

5.3 The Beneficiary shall be entitled to exercise its rights and to make demands on the Guarantor under this Deed of Guarantee as often as it wishes and the making of a demand (whether effective, partial or defective) in respect of the Default by the Supplier of any Guaranteed Obligation shall not preclude the Beneficiary from making a further demand in respect of the same or some other Default in respect of the same Guaranteed Obligation.

5.4 The Beneficiary shall not be obliged before taking steps to enforce this Deed of Guarantee against the Guarantor to obtain judgment against the Supplier or the Guarantor or any third party in any court, or to make or file any claim in a bankruptcy or liquidation of the Supplier or any third party, or to take any action whatsoever against the Supplier or the Guarantor or any third party or to resort to any other security or guarantee or other means of payment. No action (or inaction) by the Beneficiary in respect of any such security, guarantee or other means of payment shall prejudice or affect the liability of the Guarantor hereunder.

5.5 The Beneficiary's rights under this Deed of Guarantee are cumulative and not exclusive of any rights provided by law and may be exercised from time to time and as often as the Beneficiary deems expedient.

5.6 Any waiver by the Beneficiary of any terms of this Deed of Guarantee, or of any Guaranteed Obligations shall only be effective if given in writing and then only for the purpose and upon the terms and conditions, if any, on which it is given.

5.7 Any release, discharge or settlement between the Guarantor and the Beneficiary shall be conditional upon no security, disposition or payment to the Beneficiary by the Guarantor or any other person being void, set aside or ordered to be refunded pursuant to any enactment or law relating to liquidation, administration or insolvency or for any other reason whatsoever

and if such condition shall not be fulfilled the Beneficiary shall be entitled to enforce this Deed of Guarantee subsequently as if such release, discharge or settlement had not occurred and any such payment had not been made. The Beneficiary shall be entitled to retain this security after as well as before the payment, discharge or satisfaction of all monies, obligations and liabilities that are or may become due owing or incurred to the Beneficiary from the Guarantor for such period as the Beneficiary may determine.

5.8 The Guarantor shall afford any auditor of the Beneficiary appointed under the Guaranteed Agreement access to such records and accounts at the Guarantor's premises and/or provide such records and accounts or copies of the same, as may be required and agreed with any of the Beneficiary's auditors from time to time, in order that the Auditor may identify or investigate any circumstances which may impact upon the financial stability of the Guarantor.

6. GUARANTOR INTENT

Without prejudice to the generality of Clause 5 (Beneficiary's protections), the Guarantor expressly confirms that it intends that this Deed of Guarantee shall extend from time to time to any (however fundamental) variation, increase, extension or addition of or to the Guaranteed Agreement and any associated fees, costs and/or expenses.

7. RIGHTS OF SUBROGATION

7.1 The Guarantor shall, at any time when there is any Default in the performance of any of the Guaranteed Obligations by the Supplier and/or any default by the Guarantor in the performance of any of its obligations under this Deed of Guarantee, exercise any rights it may have:

7.1.1 of subrogation and indemnity;

7.1.2 to take the benefit of, share in or enforce any security or other guarantee or indemnity for the Supplier's obligations; and

7.1.3 to prove in the liquidation or insolvency of the Supplier,

only in accordance with the Beneficiary's written instructions and shall hold any amount recovered as a result of the exercise of such rights on trust for the Beneficiary and pay the same to the Beneficiary on first demand. The Guarantor hereby acknowledges that it has not taken any security from the Supplier and agrees not to do so until Beneficiary receives all moneys payable hereunder and will hold any security taken in breach of this Clause on trust for the Beneficiary.

8. DEFERRAL OF RIGHTS

8.1 Until all amounts which may be or become payable by the Supplier under or in connection with the Guaranteed Agreement have been irrevocably paid in full, the Guarantor agrees that, without the prior written consent of the Beneficiary, it will not:

8.1.1 exercise any rights it may have to be indemnified by the Supplier;

8.1.2 claim any contribution from any other guarantor of the Supplier's obligations under the Guaranteed Agreement;

8.1.3 take the benefit (in whole or in part and whether by way of subrogation or otherwise) of any rights of the Beneficiary under the Guaranteed Agreement or of any other guarantee or security taken pursuant to, or in connection with, the Guaranteed Agreement;

8.1.4 demand or accept repayment in whole or in part of any indebtedness now or hereafter due from the Supplier; or

8.1.5 claim any set-off or counterclaim against the Supplier;

8.2 If the Guarantor receives any payment or other benefit or exercises any set off or counterclaim or otherwise acts in breach of this Clause 8, anything so received and any benefit derived directly or indirectly by the Guarantor therefrom shall be held on trust for the Beneficiary and applied in or towards discharge of its obligations to the Beneficiary under this Deed of Guarantee.

9. REPRESENTATIONS AND WARRANTIES

9.1 The Guarantor hereby represents and warrants to the Beneficiary that:

9.1.1 the Guarantor is duly incorporated and is a validly existing company under the laws of its place of incorporation, has the capacity to sue or be sued in its own name and has power to carry on its business as now being conducted and to own its property and other assets;

9.1.2 the Guarantor has full power and authority to execute, deliver and perform its obligations under this Deed of Guarantee and no limitation on the powers of the Guarantor will be exceeded as a result of the Guarantor entering into this Deed of Guarantee;

9.1.3 the execution and delivery by the Guarantor of this Deed of Guarantee and the performance by the Guarantor of its obligations under this Deed of Guarantee including entry into and performance of a contract pursuant to Clause 3, have been duly authorised by all necessary corporate action and do not contravene or conflict with:

(a) the Guarantor's memorandum and articles of association or other equivalent constitutional documents;

(b) any existing law, statute, rule or regulation or any judgment, decree or permit to which the Guarantor is subject; or

(c) the terms of any agreement or other document to which the Guarantor is a Party or which is binding upon it or any of its assets;

9.1.4 all governmental and other authorisations, approvals, licences and consents, required or desirable, to enable it lawfully to enter into, exercise its rights and comply with its obligations under this Deed of Guarantee, and to make this Deed of Guarantee admissible in evidence in its jurisdiction of incorporation, have been obtained or effected and are in full force and effect; and

9.1.5 this Deed of Guarantee is the legal, valid and binding obligation of the Guarantor and is enforceable against the Guarantor in accordance with its terms.

10. PAYMENTS AND SET-OFF

10.1 All sums payable by the Guarantor under this Deed of Guarantee shall be paid without any set-off, lien or counterclaim, deduction or withholding, howsoever arising, except for those required by law, and if any deduction or withholding must be made by law, the Guarantor will pay that additional amount which is necessary to ensure that the Beneficiary receives a net amount equal to the full amount which it would have received if the payment had been made without the deduction or withholding.

10.2 The Guarantor shall pay interest on any amount due under this Deed of Guarantee at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgment.

10.3 The Guarantor will reimburse the Beneficiary for all legal and other costs (including VAT) incurred by the Beneficiary in connection with the enforcement of this Deed of Guarantee.

11. GUARANTOR'S ACKNOWLEDGEMENT

The Guarantor warrants, acknowledges and confirms to the Beneficiary that it has not entered into this Deed of Guarantee in reliance upon, nor has it been induced to enter into this Deed of Guarantee by any representation, warranty or undertaking made by or on behalf of the Beneficiary (whether express or implied and whether pursuant to statute or otherwise) which is not set out in this Deed of Guarantee.

12. ASSIGNMENT

12.1 The Beneficiary shall be entitled to assign or transfer the benefit of this Deed of Guarantee at any time to any person without the consent of the Guarantor being required and any such assignment or transfer shall not release the Guarantor from its liability under this Guarantee.

12.2 The Guarantor may not assign or transfer any of its rights and/or obligations under this Deed of Guarantee.

13. SEVERANCE

If any provision of this Deed of Guarantee is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision shall be severed and the remainder of the provisions hereof shall continue in full force and effect as if this Deed of Guarantee had been executed with the invalid, illegal or unenforceable provision eliminated.

14. THIRD PARTY RIGHTS

Other than the Beneficiary, a person who is not a Party to this Deed of Guarantee shall have no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Deed of Guarantee. This Clause does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.

15. SURVIVAL

This Deed of Guarantee shall survive termination or expiry of the Guaranteed Agreement.

16. GOVERNING LAW

16.1 This Deed of Guarantee and any non-contractual obligations arising out of or in connection with it shall be governed by and construed in all respects in accordance with English law.

16.2 The Guarantor irrevocably agrees for the benefit of the Beneficiary that the courts of England shall have jurisdiction to hear and determine any suit, action or proceedings and to settle any dispute which may arise out of or in connection with this Deed of Guarantee and for such purposes hereby irrevocably submits to the jurisdiction of such courts.

16.3 Nothing contained in this Clause shall limit the rights of the Beneficiary to take proceedings against the Guarantor in any other court of competent jurisdiction, nor shall the taking of any such proceedings in one or more jurisdictions preclude the taking of proceedings in any other jurisdiction, whether concurrently or not (unless precluded by applicable law).

16.4 The Guarantor irrevocably waives any objection which it may have now or in the future to the courts of England being nominated for the purpose of this Clause on the ground of venue or otherwise and agrees not to claim that any such court is not a convenient or appropriate forum.

16.5 The Guarantor hereby irrevocably designates, appoints and empowers [the Supplier either at its registered office from time to time to act as its authorised agent to receive notices, demands, service of process and any other legal summons in England and Wales for the purposes of any legal action or proceeding brought or to be brought by the Beneficiary in respect of this Deed of Guarantee. The Guarantor hereby irrevocably consents to the service of notices and demands, service of process or any other legal summons served in such way.]

IN WITNESS whereof the Guarantor has caused this instrument to be executed and delivered as a Deed the day and year first before written.

EXECUTED as a DEED by

[redacted] acting by [redacted]

Director [redacted]

~~Director~~/Secretary [redacted]