Trust Deed

Date

03 January 2023

FORM OF AGREEMENT

Incorporating the NEC3 Engineering and Construction Contract April 2013

Between

UK Health Security Agency

And

Barry Morgan Limited

For the provision of

Colindale - Minor Works Capital Activity

This agreement is made between the *Employer*, the *Contractor* and the Named Suppliers.

Terms in this deed have the meanings given to them in the contract between UK Health Security Agency and Barry Morgan Limited for Colindale - Minor Works Capital Activity (the *works*).

Background

The *Employer* and the *Contractor* have entered into a contract for the *works.*

The Named Suppliers have entered into contracts with the *Contractor* or a Subcontractor in connection with the *works*.

The *Contractor* has established a Project Bank Account to make provision for payment to the *Contractor* and the Named Suppliers.

Agreement

The parties to this deed agree that

- sums due to the *Contractor* and Named Suppliers and set out in the Authorisation are held in trust in the Project Bank Account by the *Contractor* for distribution to the *Contractor* and Named Suppliers in accordance with the banking arrangements applicable to the Project Bank Account,
- further Named Suppliers may be added as parties to this deed with the agreement of the *Employer* and *Contractor.* The agreement of the *Employer* and *Contractor* is treated as agreement by the Named Suppliers who are parties to this deed,
- this deed is subject to the law of the contract for the *works*,
- the benefits under this deed may not be assigned.

Executed as a deed by

Signed on behalf of UKHSA:

Signed on behalf of Barry Morgan Limited:

CONTRACT DATA

Part one – Data provided by the *Employer*

1 General

- The *conditions of contract* are the core clauses and the clauses for main Option [redacted]
- The *work*s are
- Colindale - Minor Works Capital Activity The *Employer* is

Name - UK Health Security Agency
Address 10 South Colonnade, Canary Wharf, London, E14 4PU

- The *Project Manager* is

Name . [redacted]
Address [redacted]

- The *Supervisor* is

Name . [redacted].
Address . [redacted]

- The *Adjudicator* is the person agreed by the Parties from the list of Adjudicators published by the Chartered Institute of Arbitrators or nominated by the *Adjudicator nominating body* in the absence of agreement.

- [redacted]
- [redacted]
- [redacted]

- 23_09_22_Final_C227784_ColindaleMinorWorks_PreConInf

- The *boundaries of the site* are under*:*

23_09_22_Final_C227784_ColindaleMinorWorks_PreConInf

- The *language of this contract* is English

- The *law of the contract* is the law of England and Wales, and the Courts of the country selected above, shall have exclusive jurisdiction with regard to any dispute in connection with this Agreement and the Parties irrevocably agree to submit to jurisdiction of those courts.

- The *period for reply* is two weeks.

- The *Adjudicator nominating body* is the Royal Institute of Chartered Surveyors.

- The *tribunal* is arbitration.

- The following matters will be included in the Risk Register

1. Matters raised in an initial risk reduction meeting in accordance with Core Clause 16, this meeting will serve to mutually identify matters to be included in the risk register. This initial meeting shall be held within the period of reply set out in this contract.

2. Any and all matters identified in accordance with Core Clause 16, after the initial risk reduction meeting is held.

3 Time

- [redacted]

- The *access dates* are

Part of the Site: Date

[redacted]. [redacted]

- The *Contractor* submits revised programmes at intervals no longer than 2 weeks.

4 Testing and Defects

- The *defects date* is 52 weeks after Completion of the whole of the *works*.
- The *defect correction period* is 2 weeks

5 Payment

- The *currency of this contract* is the GBP
- The *assessment interval* is 4 weeks (not more than five).
- [redacted]

6 Compensation events

- The place where weather is to be recorded is Winterbourne Gunner

- The *weather measurements* to be recorded for each calendar month are
  - the cumulative rainfall (mm)
  - the number of days with rainfall more than 5 mm
  - the number of days with minimum air temperature less than 0 degrees Celsius
  - the number of days with snow lying at 08:00 hours GMT
  - and these measurements: N/A

- The *weather measurements* are supplied by Met Office
- The *weather data* are the records of past *weather measurements* for each
- calendar month which were recorded at Winterbourne Gunner and which are available from Met Office

Where no recorded data are available

- Assumed values for the ten year return *weather data* for each *weather measurement* for each calendar month are

N/A

8 Risks and insurance

- The minimum limit of indemnity for insurance in respect of loss of or damage to property (except the *works*, Plant and Materials and Equipment) and liability for bodily injury to or death of a person (not an employee of the *Contractor*) caused by activity in connection with this contract for any one event is £5,000,000
- The minimum limit of indemnity for insurance in respect of death of or bodily injury to employees of the *Contractor* arising out of and in the course of their

employment in connection with this contract for any one event is £5,000,000

Optional statements

If the *tribunal* is arbitration

- The *arbitration procedure* is the London Court of International Arbitration Rules
- The place where arbitration is to be held is London.
- The person or organisation who will choose an arbitrator
  - if the Parties cannot agree a choice or
  - if the *arbitration procedure* does not state who selects an arbitrator is the Royal Institute of Chartered Surveyors

If the *Employer* has decided the *completion date* for the whole of the *works*

- [redacted]

If the *Employer* is not willing to take over the *works* before the Completion Date

- The *Employer* is not willing to take over the *work*s before the Completion Date. – NOT USED

If no programme is identified in part two of the Contract Data

- The *Contractor* is to submit a first programme for acceptance within 2 weeks of the Contract Date.

If the *Employer* has identified work which is to meet a stated *condition* by a *key date*

- The *key date*s and *condition*s to be met are – NOT USED

If the period in which payments are made is not three weeks and Y(UK)2 is not used

- The period within which payments are made is – NOT USED

If Y(UK)2 is used and the final date for payment is not 14 days after the date when payment is due

- The period for payment is the end of a calendar month

If there are additional *Employer*'s risks

- These are additional *Employer*'s risks – NOT USED

If the *Employer* is to provide Plant and Materials

- The insurance against loss of or damage to the *work*s, Plant and Materials is to include cover for Plant and Materials provided by the *Employer* for an amount of – NOT USED

If the *Employer* is to provide any of the insurances stated in the Insurance Table

- The *Employer* provides these insurances from the Insurance Table– NOT USED

.

If additional insurances are to be provided

- The *Employer* provides these additional insurances – NOT USED

- The *Contractor* provides these additional insurances

1. Insurance against . . . . . .
Cover/indemnity is . . . . . .
2. Insurance against . . . . . .
Cover/indemnity is . . . . . .
3. Insurance against . . . . . .
Cover/indemnity is . . . . . .

If Option X1 – NOT USED

If Option X3 – NOT USED

If Option X5 – NOT USED

If Options X5 and X6 – NOT USED

If Options X5 and X7 – NOT USED

If Option X6 – NOT USED

If Option X7 is used (but not if Option X5 is also used)

- [redacted]

If Option X12 – **NOT USED**
If Option X13 – **NOT USED**
If Option X14 – **NOT USED**

If Option X16 – is used

- The *retention free amount* is – NOT USED
- [redacted]

If Option X17 – **NOT USED**

If Option X18 is used

[redacted]

.

If Option X20 is used (but not if Option X12 is also used)

- The *incentive schedule* for Key Performance Indicators is in – NOT USED
- A report of performance against each Key Performance Indicator is provided at intervals of once per months on the Friday after the month end.

If Option Y(UK)1 - **NOT USED**

If Option Y(UK)3 – **NOT USED**

If Option Z is used

- The *additional conditions of contract* are as detailed in the appended Schedule of Amendments which is to be read and construed accordingly.

Part two – Data provided by the *Contractor*

Completion of the data in full, according to the Options chosen, is essential to create a complete contract.

Statements given in all contracts

- The *Contractor* is

  Name Barry Morgan Ltd

  Address .
- The *direct fee percentage* is
- The *subcontracted fee percentage* is
- The *working areas* are the Site and site only
- The key people are

  (2)

  Experience
- The following matters will be included in the Risk Register
  -
  - .
  -
  -

Optional statements

If the *Contractor* is to provide Works Information for his design

- The Works Information for the *Contractor*'s design is in

N/A . . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .

If a programme is to be identified in the Contract Data

- [redacted]

If the *Contractor* is to decide the *completion date* for the whole of the *works*

- [redacted]

[redacted]

If Option Y(UK)1 is used

- The *project bank* is N/A . . . . . .
- *named suppliers* are N/A . . . . . .

Data for the Shorter Schedule of Cost Components

- The *activity schedule* is [redacted] . .
- The tendered total of the Prices is [redacted]
- The percentage for people overheads is [redacted]
- The published list of Equipment is the last edition of the list published by . . . . . .
- The percentage for adjustment for Equipment in the published list is . . . . . % (state plus or minus).
- The rates for other Equipment are

Equipment	size or capacity	rate
. . . . .	. . . . .	. . . . .
. . . . .	. . . . .	. . . . .
. . . . .	. . . . .	. . . . .
. . . . .	. . . . .	. . . . .

- The hourly rates for Defined Cost of design outside the Working Areas are

category of employee	hourly rate
. . . . .	. . . . .
. . . . .	. . . . .
. . . . .	. . . . .
. . . . .	. . . . .

- The percentage for design overheads is [redacted]
- The categories of design employees whose travelling expenses to and from the Working Areas are included in Defined Cost are

. . . . . .
. . . . . .
. . . . . .
. . . . . .

Appendix 1: Schedule of Amendments to NEC3 Engineering and Construction Contract

OPTION Z2 - IDENTIFIED AND DEFINED TERMS

Insert new clause 11.3 additional defined terms.

11.3 (1) Employer Confidential Information is all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel, and contractors of the *Employer*, including all IPRs, together with all information derived from any of the above, and any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered to be confidential.

11.3 (2) Employer Data is the data, text, 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, and

- which are supplied to the *Contractor* by or on behalf of the *Employer*,
- which the *Contractor* is required to generate, process, store or transmit pursuant to this contract or
- any Personal Data for which the *Employer* is the Data Controller to the extent that such Personal Data is held or processed by the *Contractor.*

11.3 (3) Commercially Sensitive Information is the information agreed between the Parties (if any) comprising the information of a commercially sensitive nature relating to the *Contractor*, the charges for the works, its IPR or its business or which the *Contractor* has indicated to the *Employer* that, if disclosed by the *Employer*, would cause the *Contractor* significant commercial disadvantage or material financial loss.

11.3 (4) Confidential Information is the Employer's Confidential Information and/or the Contractor's Confidential Information.

11.3 (5) Contracting Body is any Contracting Body as defined in Regulation 5(2) of the Public Contracts (Works, Service and Supply) (Amendment) Regulations 2000 other than the *Employer.*

11.3 (6) Contractor's Confidential Information is any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel and contractors of the *Contractor*, including IPRs, together with all information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential, including the Commercially Sensitive Information.

11.3 (7) Crown Body is any department, office or agency of the Crown.

11.3 (8) Data Controller has the meaning given to it in the Data Protection Act 2018.

11.3 (9) DOTAS is the Disclosure of Tax avoidance Schemes rules which require a promoter of tax schemes to tell HM Revenue & Customs of any specified notable arrangements or proposals and to provide prescribed information

on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992.

11.3 (10) Environmental Information Regulations is the Environmental Information Regulations 2004 and any guidance and/or codes of practice issued by the Information Commissioner in relation to such regulations.

11.3 (11) FOIA is the Freedom of Information Act 2000 and any subordinate legislation made under this Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner in relation to such legislation.

11.3 (12) General Anti-Abuse Rule is

- the legislation in Part 5 of the Finance Act 2013 and

- any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements and to avoid national insurance contributions.

11.3 (13) Halifax Abuse Principle is the principle explained in the CJEU Case C-255/02 Halifax and others.

11.3 (14) Intellectual Property Rights or "IPRs" is

- copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information,

- applications for registration, and the right to apply for registration, for any of the rights listed in the first bullet point that are capable of being registered in any country or jurisdiction,

- all other rights having equivalent or similar effect in any country or jurisdiction and all or any goodwill relating or attached thereto.

11.3 (15) Law is any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the *Contractor* is bound to comply under the *law of the contract*.

11.3(16) An Occasion of Tax Non-Compliance is

- where any tax return of the *Contractor* submitted to a Relevant Tax Authority on or after 1 October 2012 is found on or after 1 April 2013 to be incorrect as a result of,

- A Relevant Tax Authority successfully challenging the *Contractor* under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle or

- The failure of an avoidance scheme which the *Contractor* was involved in, and which was, or should have been, notified to a Relevant Tax Authority under DOTAS or any equivalent or similar regime and

where any tax return of the *Contractor* submitted to a Relevant Tax Authority on or after 1 October 2012 gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Contract Date or to a civil penalty for fraud or evasion.

11.3 (17) Personal Data has the meaning given to it in the Data Protection Act 2018.

11.3 (18) Prohibited Act is

- to directly or indirectly offer, promise or give any person working for or engaged by the *Employer* or other Contracting Body or any other public body a financial or other advantage to
- induce that person to perform improperly a relevant function or activity or
- reward that person for improper performance of a relevant function or activity,
- to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with this contract,
- committing any offence
- under the Bribery Act 2010 (or any legislation repealed or revoked by such Act),
- under legislation or common law concerning fraudulent acts or
- defrauding, attempting to defraud or conspiring to defraud the *Employer* or
- any activity, practice or conduct which would constitute one of the offences listed above if such activity, practice or conduct had been carried out in the UK.

11.3 (19) Request for Information is a request for information or an apparent request under the Code of Practice on Access to government Information, FOIA or the Environmental Information Regulations.

11.3 (20) Relevant Requirements are all applicable laws relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State for Justice pursuant to section 9 of the Bribery Act 2010.

11.3 (21) Relevant Tax Authority is HM Revenue & Customs, or, if applicable, a tax authority in the jurisdiction in which the *Contractor* is established.

11.3 (22) Security Policy means the *Employer*'s security policy attached as Appendix 1 to Contract Schedule J (Security Provisions) as may be updated from time to time.

OPTION Z 4 - ADMITTANCE TO *SITE*

Insert new clause 19A:

19A.1 The *Contractor* submits to the *Project Manager* details of people who are to be employed by it and its Subcontractors in connection with the *works*. The details include a list of names and addresses, the capabilities in which they are employed, and other information required by the *Project Manager*.

19A.2 The *Project Manager* may instruct the *Contractor* to take measures to prevent unauthorised persons being admitted to the Site.

All of the *Contractor*'s and Subcontractor's people are to carry an *Employer's* pass and comply with all conduct requirements from the *Employer* whilst they are on the parts of the Site identified in the Works Information.

19A.4 The *Contractor* submits to the *Project Manager* for acceptance a list of the names of the people for whom passes are required. On acceptance, the *Project Manager* issues the passes to the *Contractor*. Each pass is returned to the *Project Manager* when the person no longer requires access to that part of the Site or after the *Project Manager* has given notice that the person is not to be admitted to the Site.

19A.5 The *Contractor* does not take photographs of the Site or of work carried out in connection with the *works* unless it has obtained the acceptance of the *Project Manager*.

19A.6 The *Contractor* takes the measures needed to prevent its and its Subcontractors' people taking, publishing or otherwise circulating such photographs.

OPTION Z5 - PREVENTION OF FRAUD AND BRIBERY

Insert new clauses:

18.2.1 The *Contractor* represents and warrants that neither it, nor to the best of its knowledge any of its people, have at any time prior to the Contract Date

- committed a Prohibited Act or been formally notified that it is subject to an investigation or prosecution which relates to an alleged Prohibited Act and/or

- been listed by any government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in government procurement programmes or contracts on the grounds of a Prohibited Act.

18.2.2 During the carrying out of the *works* the *Contractor* does not

- commit a Prohibited Act and/or

- do or suffer anything to be done which would cause the *Employer* or any of the *Employer's* employees, consultants, contractors, sub-contractors or agents to contravene any of the Relevant Requirements or otherwise incur any liability in relation to the Relevant Requirements.

18.2.3 During the carrying out of the *works* the *Contractor*

- establishes, maintains and enforces, and requires that its Subcontractors establish, maintain and enforce, policies and procedures which are adequate to ensure compliance with the Relevant Requirements and prevent the occurrence of a Prohibited Act,

- keeps appropriate records of its compliance with this contract and make such records available to the *Employer* on request and

- provides and maintains and where appropriate enforces an anti-bribery policy (which shall be disclosed to the *Employer* on request) to prevent it and any *Contractor's* employees or any person acting on the *Contractor's* behalf from committing a Prohibited Act.

18.2.4 The *Contractor* immediately notifies the *Employer* in writing if it becomes aware of any breach of clause

18.2.1, or has reason to believe that it has or any of its employees or Subcontractors have

- been subject to an investigation or prosecution which relates to an alleged Prohibited Act,

- been listed by any government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in government procurement programmes or contracts on the grounds of a Prohibited Act or

- received a request or demand for any undue financial or other advantage of any kind in connection with the performance of this contract or otherwise suspects that any person or Party directly or indirectly connected with this contract has committed or attempted to commit a Prohibited Act.

18.2.5 If the *Contractor* makes a notification to the *Employer* pursuant to clause 18.2.4, the *Contractor* responds promptly to the *Employer's* enquiries, co-operates with any investigation, and allows the *Employer* to audit any books, records and/or any other relevant documentation in accordance with this contract.

18.2.6 If the *Contractor* breaches Clause 18.2.3, the *Employer* may by notice require the *Contractor* to remove from carrying out the *works* any *Contractor* employee whose acts or omissions have caused the *Contractor*'s breach.

OPTION Z7 - LEGISLATION AND OFFICIAL SECRETS

Insert new clauses:

20.6 The *Contractor* complies with Law in the carrying out of the *works.*

20.7 The Official Secrets Acts 1911 to 1989 and, where appropriate, the provisions of section 11 of the Atomic Energy Act 1946 apply to this contract.

20.8 The *Contractor* notifies its people and its Subcontractors of their duties under these Acts.

OPTION Z10 - FREEDOM OF INFORMATION

Insert new clauses:

28.1 The *Contractor* acknowledges that unless the *Project Manager* has notified the *Contractor* that the *Employer* is exempt from the provisions of the FOIA, the *Employer* is subject to the requirements of the Code of Practice on Government Information, the FOIA and the Environmental Information Regulations. The *Contractor* cooperates with and assists the *Employer* so as to enable the *Employer* to comply with its information disclosure obligations.

28.2 The *Contractor*

- transfers to the *Project Manager* all Requests for Information that it receives as soon as practicable and in any event within two working days of receiving a Request for Information,

- provides the *Project Manager* with a copy of all information in its possession, or power in the form that the *Project Manager* requires within five working days (or such other period as the *Project Manager* may specify) of the *Project Manager's* request,

- provides all necessary assistance as reasonably requested by the *Project Manager* to enable the *Employer* to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations and

- procures that its Subcontractors do likewise.

28.3 The *Employer* is responsible for determining in its absolute discretion whether any information is exempt from disclosure in accordance with the provisions of the Code of Practice on Government Information, FOIA or the Environmental Information Regulations.

28.4 The *Contractor* does not respond directly to a Request for Information unless authorised to do so by the *Project Manager*.

28.5 The *Contractor* acknowledges that the *Employer* may, acting in accordance with the Department of Constitutional Affairs' Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000, be obliged to disclose information without consulting or obtaining consent from the *Contractor* or despite the *Contractor* having expressed negative views when consulted.

28.6 The *Contractor* ensures that all information is retained for disclosure throughout the *period for retention* and permits the *Project Manager* to inspect such records as and when reasonably requested from time to time.

OPTION Z13 - CONFIDENTIALITY AND INFORMATION SHARING

Insert a new clause

28.7 Except to the extent set out in this clause or where disclosure is expressly permitted elsewhere in this contract, each Party shall

- treat the other Party's Confidential Information as confidential and safeguard it accordingly,

- not disclose the other Party's Confidential Information to any other person without prior written consent,

- immediately notify the other Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information,

- notify the Serious Fraud Office where the Party has reasonable grounds to believe that the other Party is involved in activity that may be a criminal offence under the Bribery Act 2010,

28.8 The clause above shall not apply to the extent that

- such disclosure is a requirement of the Law placed upon the Party making the disclosure, including any requirements for disclosure under the FOIA or the Environmental Information Regulations pursuant to clause Z10 (Freedom of Information),

- such information was in the possession of the Party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner,

- such information was obtained from a third party without obligation of confidentiality,

- such information was already in the public domain at the time of disclosure otherwise than by a breach of this contract or

- it is independently developed without access to the other Party's Confidential Information.

28.9 The *Contractor* may only disclose the Employer*'s* Confidential Information to the people who are directly involved in the carrying out of the *works* and who need to know the information, and shall ensure that such people are aware of and shall comply with these obligations as to confidentiality.
The *Contractor* shall not, and shall procure that the *Contractor*'s people do not, use any of the Employer Confidential Information received otherwise than for the purposes of this contract.

28.10 The *Contractor* may only disclose the Employer Confidential Information to *Contractor's* people who need to know the information, and shall ensure that such people are aware of, acknowledge the importance of, and comply with these obligations as to confidentiality. In the event that any default, act or omission of any *Contractor's* people causes or contributes (or could cause or contribute) to the *Contractor* breaching its obligations as to confidentiality under or in connection with this contract, the *Contractor* shall take such action as may be appropriate in the circumstances, including the use of disciplinary procedures in serious cases. To the fullest extent permitted by its own obligations of confidentiality to any *Contractor's* people, the *Contractor* shall provide such evidence to the *Employer* as the *Employer* may reasonably require (though not so as to risk compromising or prejudicing the case) to demonstrate that the *Contractor* is taking appropriate steps to comply with this clause, including copies of any written communications to and/or from *Contractor's* people, and any minutes of meetings and any other records which provide an audit trail of any discussions or exchanges with *Contractor's* people in connection with obligations as to confidentiality.

28.11 At the written request of the *Employer*, the *Contractor* shall procure that those members of the *Contractor's* people identified in the *Employer*'s request signs a confidentiality undertaking prior to commencing any work in accordance with this contract.

28.12 Nothing in this contract shall prevent the *Employer* from disclosing the *Contractor*'s Confidential Information

- to any Crown Body or any other Contracting Bodies. All Crown Bodies or Contracting Bodies receiving such Confidential Information shall be entitled to further disclose the Confidential Information to other Crown Bodies or other Contracting Bodies on the basis that the information is confidential and is not to be disclosed to a third party which is not part of any Crown Body or any Contracting Body,

- to a professional adviser, contractor, consultant, supplier or other person engaged by the *Employer* or any Crown Body (including any benchmarking organisation) for any purpose connected with this contract, or any person conducting an Office of Government Commerce Gateway Review,

- for the purpose of the examination and certification of the *Employer*'s accounts,

- for any examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the *Employer* has used its resources,

- for the purpose of the exercise of its rights under this contract or

- to a proposed successor body of the *Employer* in connection with any assignment, novation or disposal of any of its rights, obligations or liabilities under this contract,

and for the purposes of the foregoing, disclosure of the Contractor's Confidential Information shall be on a confidential basis and subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the *Employer* under this clause 29.14.

28.13 The *Employer* shall use all reasonable endeavours to ensure that any government department, Contracting Body, people, third party or subcontractor to whom the *Contractor*'s Confidential Information is disclosed pursuant to the above clause is made aware of the *Employer*'s obligations of confidentiality.

28.14 Nothing in this clause shall prevent either party from using any techniques, ideas or know-how gained during the performance of the contract in the course of its normal business to the extent that this use does not result in a disclosure of the other party's Confidential Information or an infringement of IPR.

28.15 The *Employer* may disclose the Confidential Information of the *Contractor*

- to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement,

- to the extent that the *Employer* (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions,

OPTION Z14 - SECURITY REQUIREMENTS

The *Contractor* complies with, and procures the compliance of the *Contractor'*s people, with the Security Policy and the Security Management Plan produced by the *Contractor* and the *Contractor* shall ensure that the Security Management Plan fully complies with the Security Policy and Contract Schedule J.

OPTION Z16 - TAX COMPLIANCE

Insert new clauses:

28.16 The *Contractor* represents and warrants that at the Contract Date, it has notified the *Employer* in writing of any Occasions of Tax Non-Compliance or any litigation that it is involved in that is in connection with any Occasions of Tax Non-Compliance.

28.17 If, at any point prior to the *defects date*, an Occasion of Tax Non-Compliance occurs, the *Contractor* shall

- notify the *Employer* in writing of such fact within 5 days of its occurrence and

- promptly provide to the *Employer*

- details of the steps which the *Contractor* is taking to address the Occasions of Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant and
- such other information in relation to the Occasion of Tax Non-Compliance as the *Employer* may reasonably require.

OPTION Z20 – NOT USED - THE CONTRACTS (RIGHTS OF THIRD PARTIES) ACT 1999

OPTION Z22 - FAIR PAYMENT

Insert a new clause:

56.1 The *Contractor* assesses the amount due to a Subcontractor without taking into account the amount certified by the *Project Manager*.

56.2 The *Contractor* includes in the contract with each Subcontractor

- a period for payment of the amount due to the Subcontractor not greater than 5 days after the final date for payment in this contract. The amount due includes, but is not limited to, payment for work which the Subcontractor has completed from the previous assessment date up to the current assessment date in this contract,

- a provision requiring the Subcontractor to include in each subsubcontract the same requirement (including this requirement to flow down, except that the period for payment is to be not greater than 9 days after the final date for payment in this contract and

- a provision requiring the Subcontractor to assess the amount due to a subsubcontractor without taking into account the amount paid by the *Contractor.*

OPTION Z26 - BUILDING INFORMATION MODELLING (BIM)

21A.1 A BIM Protocol applies/does not apply [delete as appropriate]

21A.2 When a BIM Protocol applies it is detailed in the Employer's Information Requirements

21A.3 When the CIC Building Information Modelling Protocol applies clauses 21.A.4 to

21.A.6 shall apply

21A.4 In this clause, the Protocol is the CIC Building Information Modelling Protocol, second edition 2018. Terms used in this clause are those defined in the Protocol.

21A.5 Clauses 1, 2, 5, 6, 7, 8, 10 of the Protocol are *additional conditions of contract*. Clauses 3 and 4 and Appendices 1, 2 and 3 of the Protocol are Works Information.

21A.6: The following are compensation events:

- The *Contractor* encounters an event which is outside its reasonable control and which prevents it from carrying out the work specified in clauses 4.1.2 to 4.1.4 of the Protocol.

- The *Employer* revokes a licence granted under clause 6.5 of the Protocol.

OPTION Z42 - THE HOUSING GRANTS, CONSTRUCTION AND REGENERATION ACT 1996

Add an additional clause Y2.5

Y2.5 If Option Y(UK)2 is said to apply then notwithstanding that this contract relates to the carrying out of construction operations other than in England or Wales or Scotland, the Act is deemed to apply to this contract. [Guidance: for works carried out in Northern Ireland]

OPTION Z44 – INTELLECTUAL PROPERTY RIGHTS

Delete clause 22 and insert the following clause

In this clause 22 only:

"Document" means all designs, drawings, specifications, software, electronic data, photographs, plans, surveys, reports, and all other documents and/or information prepared by or on behalf of the *Contractor* in relation to this contract.

22.1 The Intellectual Property Rights in all Documents prepared by or on behalf of the *Contractor* in relation to this contract and the work executed from them remains the property of the *Contractor*. The *Contractor* hereby grants to the *Employer* an irrevocable, royalty free, non-exclusive licence to use and reproduce the Documents for any and all purposes connected with the construction, use, alterations or demolition of the *works*. Such licence entitles the *Employer* to grant sub-licences to third parties in the same terms as this licence provided always that the *Contractor* shall not be liable to any licencee for any use of the Documents or the Intellectual Property Rights in the Documents for purposes other than those for which the same were originally prepared by or on behalf of the *Contractor*.

22.2 The *Employer* may assign novate or otherwise transfer its rights and obligations under the licence granted pursuant to 22.1 to a Crown Body or to anybody (including any private sector body) which performs or carries on any functions and/or activities that previously had been performed and/or carried on by the *Employer*.

22.3 In the event that the *Contractor* does not own the copyright or any Intellectual Property Rights in any Document the *Contractor* uses all reasonable endeavours to procure the right to grant such rights to the *Employer* to use any such copyright or Intellectual Property Rights from any third party owner of the copyright or Intellectual Property Rights. In the event that the *Contractor* is unable to procure the right to grant to the *Employer* in accordance with the foregoing the *Contractor* procures that the third party grants a direct licence to the *Employer* on industry acceptable terms.

22.4 The *Contractor* waives any moral right to be identified as author of the Documents in accordance with section 77, Copyright Designs and Patents Acts 1988 and any right not to have the Documents subjected to derogatory treatment in accordance with section 8 of that Act as against the *Employer* or any licensee or assignee of the *Employer*.

22.5 In the event that any act unauthorised by the *Employer* infringes a moral right of the *Contractor* in relation to the Documents the *Contractor* undertakes, if the *Employer* so requests and at the *Employer*'s expense, to institute proceedings for infringement of the moral rights.

22.6 The *Contractor* warrants to the *Employer* that it has not granted and shall not (unless authorised by the *Employer*) grant any rights to any third party to use or otherwise exploit the Documents.

22.7 The *Contractor* supplies copies of the Documents to the *Project Manager* and to the *Employer*'s other contractors and consultants for no additional fee to the extent necessary to enable them to discharge their respective functions in relation to this contract or related works.

22.8 After the termination or conclusion of the *Contractor*'s employment hereunder, the *Contractor* supplies the *Project Manager* with copies and/or computer discs of such of the Documents as the *Project Manager* may from time to time request and the *Employer* pays the *Contractor*'s reasonable costs for producing such copies or discs.

22.9 In carrying out the *works* the *Contractor* does not infringe any Intellectual Property Rights of any third party. The *Contractor* indemnifies the *Employer* against claims, proceedings, compensation and costs arising from an infringement or alleged infringement of the Intellectual Property Rights of any third party.

OPTION Z46 - MOD DEFCON REQUIREMENTS – NOT USED

OPTION Z47 - SMALL AND MEDIUM SIZED ENTERPRISES (SMES)

Insert new clause:

26.5 The *Contractor* is required to take all reasonable steps to engage SMEs as Subcontractors and to seek to ensure that no less than the percentage of the Subcontractors stated in the Contract Data (the "SME Percentage") are SMEs or that a similar proportion of the Defined Cost is undertaken by SMEs.
The *Contractor* is required to report to the *Employer* in its regular contract management monthly reporting cycle the numbers of SMEs engaged as Subcontractors and the value of the Defined Cost of the *works* that has been undertaken by SMEs.

Where available, the *Contractor* is required to tender its Subcontracts using the same online electronic portal as was provided by the *Employer* for the purposes of tendering this contract.

The *Contractor* is to ensure that the terms and conditions used to engage Subcontractors are no less favourable than those of this contract. A reason for the *Project Manager* not accepting subcontract conditions proposed by the *Contractor* is that they are unduly disadvantageous to the Subcontractor.

OPTION Z48 - APPRENTICESHIPS

Insert new clause:

26.6 The *Contractor* takes all reasonable steps to employ apprentices, and reports to the *Employer* the numbers of apprentices employed and the wider skills training provided, during the delivery of the *works*.

The *Contractor* takes all reasonable steps to ensure that no less than a percentage of its people (agreed between the Parties) are on formal apprenticeship programmes or that a similar proportion of hours worked in delivering the *works,* (which may include support staff and Subcontractors) are provided by employees on formal apprenticeship programmes.

The *Contractor* makes available to its people and Subcontractors working on the contract, information about the Government's Apprenticeship programme and wider skills opportunities.

The *Contractor* provides any further skills training opportunities that are appropriate for its people engaged in carrying out the *works*.

The *Contractor* provides a written report detailing the following measures in its regular contract management monthly reporting cycle and is prepared to discuss apprenticeships at its regular meetings with the *Project Manager*

- the number of people during the reporting period employed on the contract, including support staff and Subcontractors,

- the number of apprentices and number of new starts on apprenticeships directly initiated through this contract,

- the percentage of all people taking part in an apprenticeship programme,

- if applicable, an explanation from the *Contractor* as to why it is not managing to meet the specified percentage target,

- actions being taken to improve the take up of apprenticeships and

- other training/skills development being undertaken by people in relation to this contract, including:

  (a) work experience placements for 14 to 16 year olds,

  (b) work experience /work trial placements for other ages,

  (c) student sandwich/gap year placements,

  (d) graduate placements,

  (e) vocational training,

  (f) basic skills training and

  (g) on site training provision/ facilities.

Option Z100 - GDPR

Insert new clause Z100 as follows:

Z100 GDPR
The *Employer* and the *Contractor* shall comply with the provisions of schedule 1.

Option Z101 – Cyber Essentials

Insert new clause Z101 as follows:

Z101 CYBER ESSENTIALS
The *Employer* and the *Contractor* shall comply with the provisions of schedule 2

SCHEDULE[Guidance: insert schedule ref here] **GDPR**

The following definitions shall apply to this Schedule [Guidance: insert schedule ref here]
Agreement : this contract;

Processor Personnel : means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Agreement

GDPR CLAUSE DEFINITIONS:
Data Protection Legislation : (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 subject to Royal Assent to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy;

Data Protection Impact Assessment : an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

Controller, Processor , Data Subject , Personal Data , Personal Data Breach , Data Protection Officer take the meaning given in the GDPR.

Data Loss Event : any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

Data Subject Request : a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

DPA 2018 : Data Protection Act 2018

GDPR : the General Data Protection Regulation (Regulation (EU) 2016/679)
Joint Controllers: where two or more Controllers jointly determine the purposes and means of processing

LED : Law Enforcement Directive (Directive (EU) 2016/680)

Protective Measures : appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Schedule [x] (Security).

Sub-processor : any third party appointed to process Personal Data on behalf of that Processor related to this Agreement

1. DATA PROTECTION

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the *Employer* is the Controller and the *Contractor* is the Processor unless otherwise specified in Schedule [X]. The only processing that the Processor is authorised to do is listed in Schedule [X] by the Controller and may not be determined by the Processor.

1.2 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

1.3 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the *works*;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

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

(a) process that Personal Data only in accordance with Schedule [X], unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures),having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule X);

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Processor's duties under this clause;

(B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data; and

(d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

(iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

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

1.5 Subject to clause 1.6, the Processor shall notify the Controller immediately if it:

(a) receives a Data Subject Request (or purported Data Subject Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

(f) becomes aware of a Data Loss Event.

1.6 The Processor's obligation to notify under clause 1.5 shall include the provision of further information to the Controller in phases, as details become available.

1.7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

(a) the Controller with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Controller following any Data Loss Event;

(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

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

(a) the Controller determines that the processing is not occasional;

(b) the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.9 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

1.10 Each Party shall designate its own data protection officer if required by the Data Protection Legislation .

1.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:

(a) notify the Controller in writing of the intended Sub-processor and processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause [X] such that they apply to the Sub-processor; and

(d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

1.12 The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

1.13 The Controller may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

1.15 Where the Parties include two or more Joint Controllers as identified in Schedule [X] in accordance with GDPR Article 26, those Parties shall enter into a Joint Controller Agreement based on the terms outlined in Schedule [Y] in replacement of Clauses 1.1-1.14 for the Personal Data under Joint Control.

Annex A - Part 2: Schedule of Processing, Personal Data and Data Subjects

SCHEDULE [X] PROCESSING, PERSONAL DATA AND DATA SUBJECTS

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

1. The contact details of the Controller's Data Protection Officer are: [Insert Contact details]

2. The contact details of the Processor's Data Protection Officer are: [Insert Contact details]

3. The Processor shall comply with any further written instructions with respect to processing by the Controller.

4. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the *Employer* is the Controller and the *Contractor* is the Processor in accordance with Clause 1.1.
Subject matter of the processing	No data processed
Duration of the processing	N/A
Nature and purposes of the processing	N/A
Type of Personal Data being Processed	N/A
Categories of Data Subject	N/A
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	N/A

SCHEDULE J

1. CONTRACT SCHEDULE J - SECURITY PROVISIONS

1.1 Definitions

For the purposes of this schedule the following terms shall have the meanings given below:

"Affiliates"	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time;
"Breach of Security"	in accordance with the Security Requirements and the Security Policy, the occurrence of: (a) any unauthorised access to or use of the works the Employer Premises, the Sites, the Contractor System and/or any ICT, information or data (including the Confidential Information and the Employer Data) used by the *Employer* and/or the *Contractor* in connection with this contract; and/or (b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Employer Data), including any copies of such information or data, used by the *Employer* and/or the *Contractor* in connection with this contract.
"Clearance"	means national security clearance and employment checks undertaken by and/or obtained from the Defence Vetting Agency;
"Contractor Equipment"	the hardware, computer and telecoms devices and equipment supplied by the *Contractor* or its Subcontractors (but not hired, leased or loaned from the *Employer*) for the carrying out of the *works*;
"Contractor Software"	software which is proprietary to the *Contractor*, including software which is or will be used by the *Contractor* for the purposes of carrying out of the *works*;
"Contractor System"	the information and communications technology system used by the *Contractor* in carrying out of the *works* including the Software, the Contractor Equipment and related cabling (but excluding the Employer System);
"Control"	means that a person possesses, directly or indirectly, the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and "Controls" and "Controlled" shall be interpreted accordingly;

"Default"	any breach of the obligations of the relevant party (including but not limited to fundamental breach or breach of a fundamental term) or any other default, act, omission, negligence or statement of the relevant party, its employees, servants, agents or Sub contractors in connection with or in relation to the subject-matter of this contract and in respect of which such party is liable to the other;
"Dispute Resolution Procedure"	the dispute resolution procedure set out in this contract (if any) or as agreed between the parties;
"Employer Premises"	means premises owned, controlled or occupied by the *Employer* or its Affiliates which are made available for use by the *Contractor* or its Subcontractors for carrying out of the *works* (or any of them) on the terms set out in this contract or any separate agreement or licence;
"Employer System"	the *Employer*'s computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the *Employer* or the *Contractor* in connection with this contract which is owned by or licensed to the *Employer* by a third party and which interfaces with the Contractor System or which is necessary for the *Employer* to receive the *works*;
"Environmental Information Regulations"	the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issues by the Information Commissioner or relevant Government Department in relation to such regulations;
"FOIA"	the Freedom of Information Act 2000 and any subordinate legislation made under this Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government Department in relation to such legislation;
"Good Industry Practice"	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;
"ICT"	information and communications technology;
"ICT Environment"	the Employer System and the Contractor System;
"Impact Assessment"	an assessment of a Compensation Event;

"Information"	has the meaning given under section 84 of the Freedom of

	Information Act 2000;
"Information Assets Register"	the register of information assets to be created and maintained by the *Contractor* throughout the carrying out of the *works* as described in the contract (if any) or as otherwise agreed between the parties;
"ISMS"	the Information Security Management System as defined by ISO/IEC 27001. The scope of the ISMS will be as agreed by the parties and will directly reflect the scope of the *works*;
"Know-How"	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know how relating to the *works* but excluding know how already in the *Contractor*'s or the *Employer*'s possession before this contract;
"List x"	means, in relation to a Subcontractor, one who has been placed on List x in accordance with Ministry of Defence guidelines and procedures, due to that Sub contractor undertaking work on its premises marked as CONFIDENTIAL or above;
"Malicious Software"	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
"Process"	has the meaning given to it under the Data Protection Legislation but, for the purposes of this contract, it shall include both manual and automatic processing;
"Protectively Marked"	shall have the meaning as set out in the Security Policy Framework.
"Regulatory Bodies"	those government departments and regulatory, statutory and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this contract or any other affairs of the *Employer* and "Regulatory Body" shall be construed accordingly;
"Request for Information"	a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations;
"Security Management Plan"	the *Contractor*'s security plan prepared pursuant to paragraph 1.5.3 of schedule J (Security Management Plan) an outline of

	which is set out in Appendix 1 of schedule J (Security Management Plan);
"Security Policy Framework"	means the Cabinet Office Security Policy Framework (available from the Cabinet Office Security Policy Division);
"Security Requirements"	means the requirements in the contract relating to security of the carrying out of the *works* (if any) or such other requirements as the *Employer* may notify to the *Contractor* from time to time;
"Security Tests"	shall have the meaning set out in Appendix 2 (Security Management Plan) [Guidance: define "Security Tests" in Security Management Plan];
"Software"	Specially Written Software, *Contractor* Software and Third Party Software;
"Specially Written Software"	any software created by the *Contractor* (or by a third party on behalf of the *Contractor*) specifically for the purposes of this contract;
"Staff Vetting Procedures"	the *Employer*'s procedures and departmental policies for the vetting of personnel whose role will involve the handling of information of a sensitive or confidential nature or the handling of information which is subject to any relevant security measures, including, but not limited to, the provisions of the Official Secrets Act 1911 to 1989;
"Statement of Applicability"	shall have the meaning set out in ISO/IEC 27001 and as agreed by the parties during the procurement phase;
"Standards"	the British or international standards, *Employer*'s internal policies and procedures, Government codes of practice and guidance together with any other specified policies or procedures referred to in this contract (if any) or as otherwise agreed by the parties; and
"Third Party Software"	software which is proprietary to any third party other than an Affiliate of the *Contractor* which is or will be used by the *Contractor* for the purposes of carrying out of the *works*;

1.2 Introduction

1.2.1 This schedule covers:

1.2.1.1 principles of protective security to be applied in carrying out of the *works*;

1.2.1.2 wider aspects of security relating to carrying out of the *works*;

1.2.1.3 the development, implementation, operation, maintenance and continual improvement of an ISMS;

1.2.1.4 the creation and maintenance of the Security Management Plan;

1.2.1.5 audit and testing of ISMS compliance with the Security Requirements;

1.2.1.6 conformance to ISO/IEC 27001 (Information Security Requirements Specification) and ISO/IEC27002 (Information Security Code of Practice) and;

1.2.1.7 obligations in the event of actual, potential or attempted breaches of security.

1.3 Principles of Security

1.3.1 The *Contractor* acknowledges that the *Employer* places great emphasis on the confidentiality, integrity and availability of information and consequently on the security provided by the ISMS.

1.3.2 The *Contractor* shall be responsible for the effective performance of the ISMS and shall at all times provide a level of security which:

1.3.2.1 is in accordance with Good Industry Practice, the *law of the contract* and this contract;

1.3.2.2 complies with the Security Policy;

1.3.2.3 complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4) available from the Cabinet Office Security Policy Division (COSPD);

1.3.2.4 meets any specific security threats to the ISMS; and

1.3.2.5 complies with ISO/IEC27001 and ISO/IEC27002 in accordance with paragraph 1.3.2 of this schedule;

1.3.2.6 complies with the Security Requirements; and

1.3.2.7 complies with the *Employer*'s ICT standards.

1.3.3 The references to standards, guidance and policies set out in paragraph 1.3.2.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, from time to time.

1.3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the *Contractor* gives an early warning to the *Project Manager* of such inconsistency immediately upon becoming aware of the same, and the *Project Manager* shall, as soon as practicable, advise the *Contractor* which provision the *Contractor* shall be required to comply with.

1.4 ISMS and Security Management Plan

1.4.1 Introduction:

(i) The *Contractor* shall develop, implement, operate, maintain and continuously improve and maintain an ISMS which will, without prejudice to paragraph 1.3.2, be accepted, by the *Project Manager*, tested in accordance with the provisions relating to testing as set out in the contract (if any) or as otherwise agreed between the Parties, periodically updated and audited in accordance with ISO/IEC 27001.

1.4.1.1 The *Contractor* shall develop and maintain a Security Management Plan in accordance with this Schedule to apply during the carrying out of the *works*.

1.4.1.2 The *Contractor* shall comply with its obligations set out in the Security Management Plan.

1.4.1.3 Both the ISMS and the Security Management Plan shall, unless otherwise specified by the *Employer*, aim to protect all aspects of the *works* and all processes associated with carrying out of the *works*, including the construction, use, alterations or demolition of the *works*, the Contractor System and any ICT, information and data (including the Employer Confidential Information and the Employer Data) to the extent used by the *Employer* or the *Contractor* in connection with this contract.

1.4.2 Development of the Security Management Plan:

1.4.2.1 Within 20 Working Days after the Contract Date and in accordance with paragraph 1.4.4 (Amendment and Revision), the *Contractor* will prepare and deliver to the *Project Manager* for acceptance a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan set out in Appendix 2 of this Part 2 of this Contract Schedule J.

1.4.2.2 If the Security Management Plan, or any subsequent revision to it in accordance with paragraph 1.4.4 (Amendment and Revision), is accepted by the *Project Manager* it will be adopted immediately and will replace the previous version of the Security Management Plan at Appendix 2 of this Part 2 of this Contract Schedule J. If the Security Management Plan is not accepted by the *Project Manager* the *Contractor* shall amend it within 10 Working Days or such other period as the parties may agree in writing of a notice of non-acceptance from the *Project Manager* and re-submit to the *Project Manager* for acceptance. The parties will use all reasonable endeavours to ensure that the acceptance process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the parties may agree in writing) from the date of its first submission to the *Project Manager*. If the *Project Manager* does not accept the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure. No acceptance to be given by the *Project Manager* pursuant to this paragraph 1.4.2.2 of this schedule may be unreasonably withheld or delayed. However any failure to accept the Security Management Plan on the grounds that it does not comply with the requirements set out in paragraph 1.4.3.4 shall be deemed to be reasonable.

1.4.3 Content of the Security Management Plan:

1.4.3.1 The Security Management Plan will set out the security measures to be implemented and maintained by the *Contractor* in relation to all aspects of the *works* and all processes associated with carrying out of the *works* and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the *works* comply with the provisions of this schedule (including the principles set out in paragraph 1.3);

1.4.3.2 The Security Management Plan (including the draft version) should also set out the plans for transiting all security arrangements and responsibilities from those in place at the Contract Date

to those incorporated in the *Contractor*'s ISMS at the date notified by the *Project Manager* to the *Contractor* for the *Contractor* to meet the full obligations of the Security Requirements.

1.4.3.3 The Security Management Plan will be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other schedules of this contract which cover specific areas included within that standard.

1.4.3.4 The Security Management Plan shall be written in plain English in language which is readily comprehensible to the staff of the *Contractor* and the *Employer* engaged in the *works* and shall only reference documents which are in the possession of the *Employer* or whose location is otherwise specified in this schedule.

1.4.4 Amendment and Revision of the ISMS and Security Management Plan:

1.4.4.1 The ISMS and Security Management Plan will be fully reviewed and updated by the *Contractor* annually or from time to time to reflect:

(a) emerging changes in Good Industry Practice;

(b) any change or proposed change to the Contractor System, the *works* and/or associated processes;

(c) any new perceived or changed security threats; and

(d) any reasonable request by the *Project Manager*.

1.4.4.2 The *Contractor* will provide the *Project Manager* with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the *Employer*. The results of the review should include, without limitation:

(a) suggested improvements to the effectiveness of the ISMS;

(b) updates to the risk assessments;

(c) proposed modifications to the procedures and controls that effect information security to respond to events that may impact on the ISMS; and

(d) suggested improvements in measuring the effectiveness of controls.

1.4.4.3 On receipt of the results of such reviews, the *Project Manager* will accept any amendments or revisions to the ISMS or

1.4.4.4 Security Management Plan in accordance with the process set out at paragraph 1.4.2.2.

1.4.4.5 Any change or amendment which the *Contractor* proposes to make to the ISMS or Security Management Plan (as a result of a *Project Manager's* request or change to the *works* or otherwise) shall be subject to the early warning procedure and shall not be implemented until accepted in writing by the *Project Manager*.

1.4.5 Testing

1.4.5.1 The *Contractor* shall conduct Security Tests of the ISMS on an annual basis or as otherwise agreed by the parties. The date, timing, content and conduct of such Security Tests shall be agreed in advance with the *Project Manager.*

1.4.5.2 The *Project Manager* shall be entitled to witness the conduct of the Security Tests. The *Contractor* shall provide the *Project Manager* with the results of such tests (in a form accepted by the *Employer* in advance) as soon as practicable after completion of each Security Test.

1.4.5.3 Without prejudice to any other right of audit or access granted to the *Employer* pursuant to this contract, the *Project Manager* and/or its authorised representatives shall be entitled, at any time and without giving notice to the *Contractor*, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the *Contractor*'s compliance with the ISMS and the Security Management Plan. The *Project Manager* may notify the *Contractor* of the results of such tests after completion of each such test. Security Tests shall be designed and implemented so as to minimise the impact on the carrying out of the *works*. If such tests adversely affect the *Contractor*'s ability to carry out the *works* in accordance with the Works Information, the *Contractor* shall be granted relief against any resultant under-performance for the period of the tests.

1.4.5.4 Where any Security Test carried out pursuant to paragraphs 1.4.5.2 or 1.4.5.3 above reveals any actual or potential Breach of Security, the *Contractor* shall promptly notify the *Project Manager* of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the *Contractor* proposes to make in order to correct such failure or weakness. Subject to the *Project Manager*'s acceptance in accordance with paragraph (i), the *Contractor* shall implement such changes to the ISMS and the Security Management Plan in accordance with the timetable agreed with the *Project Manager* or, otherwise, as soon as reasonably possible. Where the change to the ISMS or Security Management Plan is made to address a non-compliance with the Security Policy or Security Requirements, the change to the ISMS or Security Management Plan is Disallowed Cost.

1.5 Compliance with ISO/IEC 27001

1.5.1 Unless otherwise agreed by the parties, the *Contractor* shall obtain independent certification of the ISMS to ISO/IEC 27001 within 12 months of the Contract Date and shall maintain such certification until the Defects Certificate or a termination certificate has been issued.

1.5.2 In the event that paragraph 1.5.1 above applies, if certain parts of the ISMS do not conform to Good Industry Practice, or controls as described in ISO/IEC 27002 are not consistent with the Security Policy, and, as a result, the *Contractor* reasonably believes that it is not compliant with ISO/IEC 27001, the *Contractor* shall promptly notify the *Project Manager* of this and the *Employer* in its absolute discretion may waive the requirement for certification in respect of the relevant parts.

1.5.3 The *Project Manager* shall be entitled to carry out such regular security audits as may be required and in accordance with Good Industry Practice, in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001.

1.5.4 If, on the basis of evidence provided by such audits, it is the *Project Manager*'s reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 is not being achieved by the *Contractor*, then the *Project Manager* shall notify the *Contractor* of the same and give the *Contractor* a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to become compliant with the principles and practices of ISO/IEC 27001. If the *Contractor* does not become compliant within the required time then the *Project Manager* has the right to obtain an independent audit against these standards in whole or in part.

1.5.5 If, as a result of any such independent audit as described in paragraph 1.5.4 the *Contractor* is found to be non-compliant with the principles and practices of ISO/IEC 27001 then the *Contractor* shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the *Employer* in obtaining such audit.

1.6 Breach of Security

1.6.1 Either party shall give an early warning to the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

1.6.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 1.6.1, the *Contractor* shall:

1.6.2.1 immediately take all reasonable steps necessary to:

(a) remedy such breach or protect the integrity of the ISMS against any such potential or attempted breach or threat; and

(b) prevent an equivalent breach in the future.

such steps shall include any action or changes reasonably required by the *Project Manager*; and

1.6.2.2 as soon as reasonably practicable provide to the *Project Manager* full details (using such reporting mechanism as defined by the ISMS) of the Breach of Security or the potential or attempted Breach of Security.

Appendix 1 – Security Policy

[Guidance Note: Append Security Policy]

APPENDIX 2 – SECURITY MANAGEMENT PLAN

[Guidance Note: Append Security Management Plan]

SCHEDULE 2 CYBER ESSENTIALS

CYBER ESSENTIALS SCHEME

1. DEFINITIONS

1.1 In this Schedule, the following words shall have the following meanings:

"Cyber Essentials Scheme"	the Cyber Essentials Scheme developed by the Government which provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet based threats (as may be amended from time to time). Details of the Cyber Essentials Scheme can be found here: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview;
"Cyber Essentials Basic Certificate"	the certificate awarded on the basis of self-assessment, verified by an independent certification body, under the Cyber Essentials Scheme and is the basic level of assurance;
"Cyber Essentials Certificate"	Cyber Essentials Basic Certificate, the Cyber Essentials Plus Certificate or the Cyber Essential Scheme certificate equivalent to be provided by the Contractor as set out in the Framework Data Sheet;
"Cyber Essential Scheme Data"	sensitive and personal information and other relevant information as referred to in the Cyber Essentials Scheme; and
"Cyber Essentials Plus Certificate"	the certification awarded on the basis of external testing by an independent certification body of the Contractor's cyber security approach under the Cyber Essentials Scheme and is a more advanced level of assurance.

2. CYBER ESSENTIALS OBLIGATIONS

2.1 Where the Works Information requires that the *Contractor* provide a Cyber Essentials Certificate prior to the execution of the *works* the *Contractor* shall provide a valid Cyber Essentials Certificate, then on or prior to the commencement of the *works* the *Contractor* delivers to the *Employer* evidence of the same. Where the *Contractor* fails to comply with this paragraph it shall be prohibited from commencing the carrying out of the *works* under any contract until such time as the *Contractor* has evidenced to the *Employer* its compliance with this paragraph 2.1.

2.2 Where the *Contractor* continues to Process Cyber Essentials Scheme Data during the carrying out of the *works* the *Contractor* delivers to the *Employer* evidence of renewal of the Cyber Essentials Certificate on each anniversary of the first applicable certificate obtained by the *Contractor* under paragraph 2.1.

2.3 Where the *Contractor* is due to Process Cyber Essentials Scheme Data after the commencement of the *works* but before completion of the *works* the *Contractor* delivers to the *Employer* evidence of:

2.3.1 a valid and current Cyber Essentials Certificate before the *Contractor* Processes any such Cyber Essentials Scheme Data; and

2.3.2 renewal of the valid Cyber Essentials Certificate on each anniversary of the first Cyber Essentials Scheme certificate obtained by the *Contractor* under paragraph 2.1.

2.4 In the event that the *Contractor* fails to comply with paragraphs 2.2 or 2.3 (as applicable), the *Employer* reserves the right to terminate this contract for material Default.

2.5 The *Contractor* ensures that all sub-contracts with Sub-Contractors who Process Cyber Essentials Data contain provisions no less onerous on the Sub-Contractors than those imposed on the *Contractor* under this contract in respect of the Cyber Essentials Scheme under paragraph 2.1 of this Schedule

2.6 This Schedule shall survive termination or expiry of this contract.