Ministry of Justice

Date: 29 March 2022

A Contract for Services

Between

The Secretary of State for Justice

And

Langley House Trust

CONTENTS

Schedules

This contract is dated:

PARTIES:

(1) THE SECRETARY OF STATE FOR JUSTICE of 102 Petty France, London, SW1H 9AJ acting as part of the Crown (the "**Authority**");

AND

(2) LANGLEY HOUSE TRUST a Private Limited Company by guarantee without share capital (registered company number 7888191)) whose registered office is 3 & 4 The Square, Manfield Avenue, Walsgrave, Coventry, England, CV2 2QJ (the "**Supplier**")

(each a "**Party**" and together the "**Parties**").

WHEREAS

The Authority wishes to appoint the Supplier to provide Move-on Accommodation and support Services for people under probation supervision with complex needs and risks, often on release from custody or upon leaving Approved Premises and the Supplier agrees to provide those services in accordance with these terms and conditions;

NOW IT IS HEREBY AGREED:

A GENERAL

A1 Definitions and Interpretation

Unless the context otherwise requires the following terms shall have the meanings given to them below:

"**Affected Party**" means the Party seeking to claim relief in respect of a Force Majeure Event.

"**Affiliate**" means 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.

"**Approval**" and "**Approved**" means the prior written consent of the Authority.

"**Associated Person**" means as it is defined in section 44(4) of the Criminal Finances Act 2017.

"**Authorised Representative**" means the Authority representative named in a CCN as authorised to approve Changes.

"**Authority Contract Manager**" means Redacted Under FOIA Section 40, the Senior Contract Manager for Her Majesty's Prison and Probation Service (HMPPS), or any subsequent Senior Contract Manager appointed by the Authority to manage the day-to-day running of the Contract on the Authority's behalf.

"**Authority Data**" means:

(a) 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: (i) supplied to the Supplier by or on behalf of the Authority; or (ii) which the Supplier is required to generate, process, store or transmit pursuant to the Contract; or

(b) any Personal Data for which the Authority is the Controller, separate to offender Personal Data.

For the avoidance of doubt, such data would include all performance data and contract information related to the delivery of Services (e.g. performance reports, staff lists, meeting information) but would exclude Offender Personal Data and Staff Personal Data.

"**Authority Premises**" means any premises owned, occupied or controlled by the Authority or any other Crown Body which are made available for use by the Supplier or its Sub-Contractors for provision of the Services.

"**Authority Software**" means software which is owned by or licensed to the Authority (other than under or pursuant to the Contract) and which is or will be used by the Supplier for the purposes of providing the Services.

"**Authority System**" means the Authority's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Authority or the Supplier in connection with the Contract which is owned by or licensed to the Authority by a third party and which interfaces with the Supplier System or which is necessary for the Authority to receive the Services.

"**Baseline Security Requirements**" means the security requirements in Annex 1 of Schedule 6.

"**BPSS**" means the Government's Baseline Personnel Security Standard for Government employees.

"**Breach of Security**" means an occurrence of:

(a) any unauthorised access to or use of the ICT Environment and/or any Information Assets and/or Authority Data (including Confidential Information) in connection with the Contract;

(b) the loss (physical or otherwise) and/or unauthorised disclosure of any Information Assets and/or Authority Data (including Confidential Information) in connection with the Contract, including copies; and/or

(c) any part of the Supplier System ceasing to be compliant with the Certification Requirements

"**BS 8555**" means the standard published to help organisations improve their environmental performance by the British Standards Institution.

"**CCN**" means a change control notice in the form set out in Schedule 3.

"**Certification Requirements**" means the requirements set out in paragraph 5.1 of Schedule 6.

"**Change**" means a change in any of the terms or conditions of the Contract.

"**Change in Law**" means any change in Law which affects the performance of the Services which comes into force after the Commencement Date.

"**Commencement Date**" means the date specified in clause A5.1.

"**Commercially Sensitive Information**" means the information listed in Schedule 4 comprising the information of a commercially sensitive nature relating to:

(a) the Price; and/or

(b) the Supplier's business and investment plans

which the Supplier has informed the Authority would cause the Supplier significant commercial disadvantage or material financial loss if it was disclosed.

"**Comparable Supply**" means the supply of services to another customer of the Supplier which are the same or similar to any of the Services.

"**Confidential Information**" means any information which has been designated as confidential by either Party in writing or that ought to be considered as confidential (however it is conveyed or on whatever media it is stored) including information the disclosure of which would, or would be likely to, prejudice the commercial interests of any person or trade secrets or Intellectual Property Rights of either Party and all Personal Data. Confidential Information shall not include information which:

(a) was public knowledge at the time of disclosure otherwise than by breach of clause E4;

(b) was in the possession of the receiving Party, without restriction as to its disclosure, before receiving it from the disclosing Party;

(c) is received from a third party (who lawfully acquired it) without restriction as to its disclosure; or

(d) is independently developed without access to the Confidential Information.

"**Contract**" means these terms and conditions, the attached Schedules and any other provisions the Parties expressly agree are included.

"**Contracting Authority**" means any contracting authority (other than the Authority) as defined in regulation 3 of the Regulations.

"**Contracts Finder**" means the Government's portal for public sector procurement opportunities.

"**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**" are interpreted accordingly.

"**Controller**" means, where Personal Data is being processed for Law Enforcement Purposes, as it is defined in the LED; and in all other circumstances, as it is defined in GDPR.

"**Copyright**" means as it is defined in s.1 of Part 1 Chapter 1 of the Copyright, Designs and Patents Act 1988.

"**Crown**" means the government of the United Kingdom (including the Northern Ireland Executive Committee and Northern Ireland Departments, the Scottish Executive and the National Assembly for Wales), including, but not limited to, Government ministers, Government departments, Government offices and Government agencies and "**Crown Body**" is an emanation of the foregoing.

"**Data Loss Event**" means any event which results, or may result, in unauthorised access to Personal Data held by the Supplier under the Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of the Contract, including any Personal Data.

"**Data Protection Impact Assessment**" means an assessment by the Controller of the effect of the envisaged processing on the protection of Personal Data.

"**Data Protection Legislation**" means:

(a) the GDPR, the LED and applicable implementing Laws;

(b) the DPA to the extent that it relates to the processing of Personal Data and privacy;

(c) all applicable Laws relating to the processing of Personal Data and privacy.

"**Data Protection Officer**" means as it is defined in the GDPR.

"**Data Subject**" means as it is defined in the GDPR.

"**Data Subject Request**" means 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.

"**Database Rights**" means as rights in databases are defined in s.3A of Part 1 Chapter 1 of the Copyright, Designs and Patents Act 1988.

"**Default**" means any breach of the obligations or warranties of the relevant Party (including abandonment of the Contract in breach of its terms, repudiatory breach or breach of a fundamental term) or any other default, act, omission, negligence or statement of the relevant Party or the Staff in connection with the subject-matter of the Contract and in respect of which such Party is liable to the other.

"**DOTAS**" means the Disclosure of Tax Avoidance Schemes rules which require a promotor of tax schemes to tell HMRC of any specified notifiable 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 and as extended to NICs by the National Insurance (Application of Part 7 of the Finance Act 2004) regulations 2012, SI 2012/1868 made under section 132A of the Social Security Administration Act 1992.

"**DPA**" means the Data Protection Act 2018.

"**EIR**" means the Environmental Information Regulations 2004 (SI 2004/3391) and any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such regulations.

"**End Date**" means the date specified in clause A5.1.

"**Equipment**" means the Supplier's equipment, consumables, plant, materials and such other items supplied and used by the Supplier in the delivery of the Services.

"**Exit Day**" means as it is defined in the European Union (Withdrawal) Act 2018.

"**Extension**" means as it is defined in clause A5.2.

"**Financial Year**" means the period from 1st April each year to the 31st March the following year.

"**FOIA**" means the Freedom of Information Act 2000 and any subordinate legislation made under that 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.

"**Force Majeure Event**" means any event outside the reasonable control of either Party affecting its performance of its obligations under the Contract arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party, including acts of God, riots, war or armed conflict, acts of terrorism, acts of Government, local government or regulatory bodies, for flood, storm or earthquake, or disaster but excluding any industrial dispute relating to the Supplier or the Staff or any other failure in the Supplier's supply chain caused by the Covid 19 pandemic or the United Kingdom's exit from the EU.

"**GDPR**" means the retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679), as transposed into UK Law by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419).

"**General Anti-Abuse Rule**" means:

(d) the legislation in Part 5 of the Finance Act 2013; and

(e) any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements to avoid NICs.

"**General Change in Law**" means a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply.

"**Good Industry Practice**" means standards, practices, methods and procedures conforming to the Law and the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar type of undertaking under the same or similar circumstances.

"**Government**" means the government of the United Kingdom.

"**Government Buying Standards**" means the standards published here:

https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs

"**Greening Government Commitments**" means the Government's policy to reduce its effects on the environment, the details of which are published here:

https://www.gov.uk/government/collections/greening-government-commitments

"**Halifax Abuse Principle**" means the principle explained in the CJEU Case C-255/02 Halifax and others.

"**HMRC**" means HM Revenue & Customs.

"**House Rules**" means the Redacted Under FOIA Section 43 set of rules in use at each property for the management of residents and the rules and procedures that the residents are obliged to comply with. These rules can be found at Appendix 1A of Schedule 1 and will be shared with the Offender Manager.

"**ICT Environment**" means the Authority System and the Supplier System.

"**Information**" has the meaning given under section 84 of the FOIA.

"**Information Assets**" means definable pieces of information stored in any manner which are determined by the Authority to be valuable and relevant to the Services.

"**Initial Term**" means the period from the Commencement Date to the End Date.

"**Intellectual Property Rights**" means patents, utility models, inventions, trademarks, service marks, logos, design rights (whether registrable or otherwise), applications for any of the foregoing, copyright, database rights, domain names, plant variety rights, Know-How, trade or business names, moral rights and other similar rights or obligations whether registrable or not in any country (including but not limited to the United Kingdom) and the right to sue for passing off.

"**ISMS**" means the Supplier's information and management system and processes to manage information security as set out in paragraph 2.3 of Schedule 6.

"**ISO 14001**" means the family of standards related to environmental management published by the International Organisation for Standardisation.

"**IT Health Check**" means penetration testing of systems under the Supplier's control on which Information Assets and/or Authority Data are held which are carried out by third parties in accordance with the CHECK scheme operated by NCSC or to an equivalent standard.

"**ITEPA**" means the Income Tax (Earnings and Pensions) Act 2003.

"**Know-How**" means all information not in the public domain held in any form (including without limitation that comprised in or derived from drawings, data formulae, patterns, specifications, notes, samples, chemical compounds, biological materials, computer software, component lists, instructions, manuals, brochures, catalogues and process descriptions and scientific approaches and methods).

"**Law**" means 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, regulatory policy, mandatory guidance or code of practice,

judgment of a relevant court of law, or directives or requirements with which the Supplier is bound to comply.

"**Law Enforcement Purposes**" means as it is defined in the DPA.

"**LED**" means the Law Enforcement Directive (Directive (EU) 2016/680).

"**Losses**" means losses, liabilities, damages, costs, fines and expenses (including legal fees on a solicitor/client basis) and disbursements and costs of investigation, litigation, settlement, judgment interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty or otherwise.

"**Malicious Software**" means 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.

"**Material Breach**" means a breach (including an anticipatory breach) that is serious in the widest sense of having a serious effect on the benefit which the Authority would otherwise derive from:

(a) a substantial portion of the Contract; or

(b) any of the obligations set out in clauses D1, D2, D3, D4, G3, I4 or paragraph 9 of Schedule 8.

"**Modern Slavery Helpline**" means the point of contact for reporting suspicion, seeking help or advice and information on the subject of modern slavery available by telephone on 08000 121 700 or online at:

https://www.modernslaveryhelpline.org/report

"**Month**" means calendar month.

"**MSA**" means the Modern Slavery Act 2015.

"NCSC" means National Cyber Security Centre

"**NICs**" means National Insurance Contributions.

"**Occasion of Tax Non-Compliance**" means:

(a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which is found on or after 1 April 2013 to be incorrect as a result of:

i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse principle or under any tax rules or legislation that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle;

ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to the Relevant Tax Authority under the DOTAS or any equivalent or similar regime; and/or

(b) any tax return of the Supplier 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 Commencement Date or to a civil penalty for fraud or evasion.

"**Offender Personal Data**" means all 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 created, processed or shared during operation of the Services regarding individual offender referrals.

"**Personal Data**" means as it is defined in the GDPR.

"**Personal Data Breach**" means as it is defined in the GDPR.

"**Premises**" means the location where the Services are to be supplied as set out in the Specification.

"**Price**" means the price (excluding any applicable VAT) payable to the Supplier by the Authority under the Contract, as set out in Schedule 2 for the full and proper performance by the Supplier of its obligations under the Contract.

"**Processor**" means, where Personal Data is being processed for Law Enforcement Purposes, as it is defined in the LED; and in all other circumstances, as it is defined in GDPR.

"**Prohibited Act**" means:

(a) to directly or indirectly offer, promise or give any person working for or engaged by the Authority a financial or other advantage to:

i) induce that person to perform improperly a relevant function or activity; or

ii) reward that person for improper performance of a relevant function or activity;

(b) 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 the Contract;

(c) an offence:

i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act;

ii) under legislation or common law concerning fraudulent acts (including offences by the Supplier under Part 3 of the Criminal Finances Act 2017); or

iii) the defrauding, attempting to defraud or conspiring to defraud the Authority;

(d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct has been carried out in the UK.

"**Property**" means the property, other than real property, owned by the Authority and made available to the Supplier by the Authority in connection with the Contract. Property includes but is not limited to physical equipment, materials and documentation.

"**Protective Measures**" means 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 measures adopted.

"**PSI 67/2011**" is the Prison Service Instruction published on 1st November 2011 relating to the searching of the person as amended from time to time and available at:

https://www.justice.gov.uk/offenders/psis/prison-service-instructions-2011

"**PSI 10/2012**" is the Prison Service Instruction published on 26 March 2012 relating to the Conveyance and Possession of Prohibited Items and other Related Offences as amended from time to time and available at:

https://www.justice.gov.uk/offenders/psis/prison-service-instructions-2012

"**PSI 07/2014**" is the Prison Service Instruction published on 2nd June 2014 relating to security vetting as amended from time to time and available at:

https://www.justice.gov.uk/offenders/psis/prison-service-instructions-2014

"**PSI 24/2014**" is the Prison Service Instruction published on 1st May 2014 relating to information assurance as amended from time to time and available at:

https://www.justice.gov.uk/offenders/psis/prison-service-instructions-2014

"**Purchase Order**" the Authority's order for the supply of the Services.

"**Quality Standards**" means the quality standards published by BSI British Standards, the National Standards Body of the United Kingdom, the International Organisation for Standardization or other reputable or equivalent body (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with, and as may be further detailed in Schedule 1.

"**Receipt**" means the physical or electronic arrival of the invoice at the address in clause C1.13 or at any other address given by the Authority to the Supplier for the submission of invoices from time to time.

"**Regulations**" means the Public Contract Regulations 2015 (SI 2015/102).

"**Regulator Correspondence**" means any correspondence from the Information Commissioner's Office, or any successor body, in relation to the processing of Personal Data under the Contract.

"**Regulatory Body**" means a Government department and regulatory, statutory and other entities, committees, ombudsmen 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 the Contract or any other affairs of the Authority.

"**Relevant Conviction**" means a conviction that is relevant to the nature of the Services or as listed by the Authority and/or relevant to the work of the Authority.

"**Relevant Requirements**" means all applicable Law 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.

"**Relevant Tax Authority**" means HMRC or, if applicable, a tax authority in the jurisdiction in which the Supplier is established.

"**Replacement Supplier**" means any third-party supplier appointed by the Authority to supply any services which are substantially similar to any of the Services in substitution for any of the Services following the expiry, termination or partial termination of the Contract.

"**Request for Information**" means a request for information under the FOIA or the EIR.

"**Results**" means any guidance, specifications, reports, studies, instructions, toolkits, plans, data, drawings, databases, patents, patterns, models, designs or other material which is:

a) prepared by or for the Supplier for use in relation to the performance of its obligations under the Contract; or

b) the result of any work done by the Supplier or any Staff in relation to the provision of the Services.

"**Returning Employees**" means those persons agreed by the Parties to be employed by the Supplier (and/or any Sub-Contractor) wholly or mainly in the supply of the Services immediately before the end of the Term.

"**Security Plan**" means the plan prepared by the Supplier which includes the matters in paragraph 3.2 of Schedule 6.

"**Security Policy Framework**" means the Government's Security Policy Framework (available from the Cabinet Office's Government Security Secretariat) as updated from time to time.

"**Security Test**" means a test carried out by the Supplier, the Authority or a third party to validate the ISMS and the security of all relevant processes and systems on which Information Assets and/or Authority Data are held.

"**Services**" means the services set out in Schedule 1 (including any modified or alternative services).

"**SME**" means an enterprise falling within the category of micro, small and medium-sized enterprises defined by the European Commission's Recommendation of 6 May 2003 available at:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF

"**Specific Change in Law**" means a Change in Law that relates specifically to the business of the Authority and which would not affect a Comparable Supply.

"**Specification**" means the description of the Services to be supplied under the Contract as set out in Schedule 1 including, where appropriate, the Quality Standards.

"**SSCBA**" means the Social Security Contributions and Benefits Act 1992.

"**Staff**" means all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any of its Sub-Contractors engaged in the performance of the Supplier's obligations under the Contract.

"**Staff Personal Data**" means all 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 created by the Supplier in the operation of the Services regarding their Staff.

"**Sub–Contract**" means a contract between two or more suppliers, at any stage of remoteness from the Authority in a sub-contracting chain, made wholly or substantially for the purpose of performing (or contributing to the performance of) the whole or any part of the Contract and "**Sub-Contractor**" shall be construed accordingly.

"**Sub-processor**" means any third party appointed to process Personal Data on behalf of the Supplier related to the Contract.

"**Supplier Software**" means software which is proprietary to the Supplier, including software which is or will be used by the Supplier for the purposes of providing the Services and which is set out in Schedule 5.

"**Supplier System**" means the information and communications technology system used by the Supplier in performing the Services including the Software, the Equipment and related cabling (but excluding the Authority System).

"**Tender**" means the Supplier's tender submitted in response to the Authority's invitation to suppliers for offers to supply the Services.

"**Term**" means the period from the Commencement Date to:

(a) the End Date; or

(b) following an Extension, the end date of the Extension

or such earlier date of termination or partial termination of the Contract in accordance with the Law or the Contract.

"**TFEU**" means the Treaty on the Functioning of the European Union.

"**Third Party IP Claim**" has the meaning given to it in clause E8.5.

"**Third Party Software**" means software which is proprietary to any third party which is or will be used by the Supplier to provide the Services including the software and which is specified as such in Schedule 5.

"**Treaties**" means the TFEU and the Treaty on European Union.

"**TUPE**" means the Transfer of Undertakings (Protection of Employment) Regulations 2006.

"**TUPE Information**" means the information set out in clause B10.1.

"**Valid Invoice**" means an invoice containing the information set out in clause C1.3 or C1.4.

"**VAT**" means value added tax charged or regulated in accordance with the Value-Added Tax Act 1994.

"**VCSE**" means a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives.

"**Vulnerability Correction Plan**" means a remedial plan prepared by the Supplier to address vulnerabilities identified in an IT Health Check report.

"**Welsh Language Scheme**" means the Authority's Welsh language scheme as amended from time to time and available at:

http://www.justice.gov.uk/publications/corporate-reports/moj/2010/welsh-language-scheme

"**Working Day**" means a day (other than a Saturday or Sunday) on which banks are open for general business in the City of London.

In the Contract, unless the context implies otherwise:

(a) the singular includes the plural and vice versa unless the context requires otherwise;

(b) words importing the masculine include the feminine and the neuter;

(c) reference to a clause is a reference to the whole of that clause unless stated otherwise;

(d) references to a person include natural persons, a company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or central Government body;

(e) the words "other", "in particular", "for example", "including" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "without limitation";

(f) headings are included for ease of reference only and shall not affect the interpretation or construction of the Contract;

(g) the Schedules form an integral part of the Contract and have effect as if set out in full in the body of the Contract. A reference to the Contract includes the Schedules;

(h) a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;

(i) references to the Contract are references to the Contract as amended from time to time;

(j) any reference in the Contract which immediately before Exit Day is a reference to (as it has effect from time to time):

(i) any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement ("EU References") which is to form part of domestic law by the application of s.3 of the European Union (Withdrawal) Act 2018 shall be read on and after Exit Day as a reference to the EU References as they form part of domestic law by virtue of s.3 of the European Union (Withdrawal) Act 2018 as modified by domestic law from time to time; and

(ii) any EU institution or EU authority or other such EU body shall be read on and after Exit Day as a reference to the UK institution, authority or body to which its functions were transferred.

A2 Authority Obligations

Save as otherwise expressly provided, the Authority's obligations under the Contract are the Authority's obligations in its capacity as a contracting counterparty and nothing in the Contract operates as an obligation upon, or in any other way fetters or constrains, the Authority in any other capacity.

A3 Supplier's Status

A3.1 The Supplier is an independent contractor and nothing in the Contract creates a contract of employment, a relationship of agency or partnership or a joint venture between the Parties and accordingly neither Party is authorised to act in the name of, or on behalf of, or otherwise bind the other Party save as expressly permitted by the Contract.

A3.2 The Supplier shall not (and shall ensure that any other person engaged in relation to the Contract shall not) say or do anything that might lead another person to believe that the Supplier is acting as the agent or employee of the Authority.

A4 Mistakes in Information

The Supplier is responsible for the accuracy of all drawings, documentation and information supplied to the Authority by the Supplier in connection with the Services and shall pay the Authority any extra costs occasioned by any discrepancies, errors or omissions therein.

A5 Term

A5.1 The Contract starts on 1st April 2022 (the "**Commencement Date**") and ends on 31st March 2025 (the "**End Date**") unless it is terminated early or extended in accordance with the Contract.

B. THE SERVICES

B1 Basis of the Contract

B1.1 In consideration of the Supplier's performance of its obligations under the Contract the Authority shall pay the Supplier the Price in accordance with clause C1.

B1.2 The terms and conditions in the Contract apply to the exclusion of any other terms and conditions the Supplier seeks to impose or incorporate, or which are implied by trade, custom, practice or course of dealing.

B2 Delivery of the Services

B2.1 The Supplier shall at all times comply with the Quality Standards and, where applicable, shall maintain accreditation with the relevant Quality Standards authorisation body. To the extent that the standard of the Service has not been specified in the Contract, the Supplier shall

agree the relevant standard of the Services with the Authority prior to the supply of the Services and, in any event, the Supplier shall perform its obligations under the Contract in accordance with the Law and Good Industry Practice.

B2.2 The Supplier acknowledges that the Authority relies on the skill and judgment of the Supplier in the supply of the Services and the performance of the Supplier's obligations under the Contract.

B2.3 The Supplier shall:

(a) ensure that all Staff supplying the Services do so with all due skill, care and diligence and shall possess such qualifications, skills and experience as are necessary for the proper supply of the Services;

(b) ensure that all Staff are properly managed and supervised; and

(c) comply with the standards and requirements set out in Schedule 8.

B2.4 Not used

B2.5 Not used

B2.6 Not used

B2.7 Not used

B2.8 The Authority may inspect the manner in which the Supplier delivers the Services at the Premises during normal business hours on reasonable notice.

B2.9 If reasonably requested to do so by the Authority, the Supplier shall co-ordinate its activities in supplying the Services with those of the Authority and other contractors engaged by the Authority.

B2.10 Timely supply of the Services is of the essence of the Contract, including in relation to commencing the supply of the Services within the time agreed or on a specified date. If the Supplier fails to supply the Services within the time promised or specified in the Specification, the Authority is released from any obligation to pay for the Services and may terminate the Contract, in either case without prejudice to any other rights and remedies of the Authority.

B2.11 If the Authority informs the Supplier in writing that the Authority reasonably believes that any part of the Services do not meet the requirements of the Contract or differs in any way from those requirements, and this is not as a result of a default by the Authority, the Supplier shall at its own expense re-schedule and carry out the Services in accordance with the requirements of the Contract within such reasonable time as may be specified by the Authority.

B2.12 If, in delivering the Services, the Supplier is required to visit Authority Premises which are prisons, the Supplier shall comply with Schedule 7.

B3 Equipment

B3.1 The Supplier shall provide all the Equipment and resource necessary for the supply of the Services.

B3.2 Not used

B3.3 All Equipment brought onto the Premises is at the Supplier's own risk and the Authority has no liability for any loss of or damage to any Equipment unless the Supplier demonstrates that such loss or damage was caused or contributed to by the Authority's Default. The Supplier shall provide for the haulage or carriage thereof to the Premises and the removal of Equipment when no longer required at its sole cost.

B3.4 Equipment brought onto the Premises remains the property of the Supplier.

B3.5 Not used

B3.6The Supplier shall maintain all Equipment in a safe, serviceable and clean condition.

B3.7 Not used

B3.8 Not used

B4 Not used

B5 Staff

B5.1 The Authority may, by notice to the Supplier, refuse to admit onto, or withdraw permission to remain on, the Authority's Premises:

(a) any member of the Staff; or

(b) any person employed or engaged by any member of the Staff

whose admission or continued presence would, in the Authority's reasonable opinion, be undesirable.

B5.2 The Authority shall maintain the security of the Authority's Premises in accordance with its standard security requirements, including Prison Rules 1999 Part III, the Prison (Amendment) Rules 2005, the Young Offender Institute Rules 2000 Part III and the Young Offender Institute (Amendment) Rules 2008, available to the Supplier on request. The Supplier shall comply with all security requirements of the Authority while on the Authority's Premises, and ensure that all Staff comply with such requirements.

B5.3 The Authority may search any persons or vehicles engaged or used by the Supplier at the Authority's Premises.

B5.4 At the Authority's written request, the Supplier shall, at its own cost, provide a list of the names, addresses, national insurance numbers and immigration status of all people who may require admission to the Authority's Premises, specifying the capacities in which they are concerned with the Contract and giving such other particulars as the Authority may reasonably request.

B5.5 The Supplier shall ensure that all Staff who have access to the Authority's Premises, the Authority System or the Authority Data have been cleared in accordance with the BPSS.

B5.6 The Supplier shall co-operate with any investigation relating to security carried out by the Authority or on behalf of the Authority and, at the Authority's request:

(a) use reasonable endeavours to make available any Staff requested by the Authority to attend an interview for the purpose of an investigation; and

(b) provide documents, records or other material in whatever form which the Authority may reasonably request or which may be requested on the Authority's behalf, for the purposes of an investigation.

B5.7 The Supplier shall comply with PSI 10/2012 as amended from time to time and available from the Authority on request.

B6 Due Diligence

B6.1 Save as the Authority may otherwise direct, the Supplier is deemed to have completed due diligence in relation to all matters connected with the performance of its obligations under the Contract.

B7 Not used

B8 Property

B8.1 All Property is and remains the property of the Authority and the Supplier irrevocably licenses the Authority and its agents to enter any Premises of the Supplier during normal business hours on reasonable notice to recover any such Property.

B8.2 The Supplier does not have a lien or any other interest on the Property and the Supplier at all times possesses the Property as fiduciary agent and bailee of the Authority. The Supplier shall take all reasonable steps to ensure that the title of the Authority to the Property and the exclusion of any such lien or other interest are brought to the notice of all Sub-Contractors and other appropriate persons and shall, at the Authority's request, store the Property separately and ensure that it is clearly identifiable as belonging to the Authority.

B8.3 The Property is deemed to be in good condition when received by or on behalf of the Supplier unless the Supplier notifies the Authority otherwise within 5 Working Days of receipt.

B8.4 The Supplier shall maintain the Property in good order and condition (excluding fair wear and tear), and shall use the Property solely in connection with the Contract and for no other purpose without Approval.

B8.5 The Supplier shall ensure the security of all the Property whilst in its possession, either on the Premises or elsewhere during the supply of the Services, in accordance with the Authority's reasonable security requirements as required from time to time.

B8.6 The Supplier is liable for all loss of or damage to the Property, unless such loss or damage was caused by the Authority's negligence. The Supplier shall inform the Authority immediately of becoming aware of any defects appearing in, or losses or damage occurring to, the Property.

B9 Offers of Employment

B9.1 Neither Party shall, directly or indirectly, solicit or procure (otherwise than by general advertising or under TUPE, any employees or contractors (including the Staff) of the other Party who are directly employed or engaged in connection with the provision of the Services while such persons are employed or engaged and for a period of 6 Months thereafter.

B9.2 If either Party breaches the clause B9.1, it shall pay the other Party a sum equivalent to 20% of the annual base salary payable by the Party in breach in respect of the first year of person's employment.

B9.3 The Parties agree that the sum specified in clause B9.2 is a reasonable pre-estimate of the loss and damage which the Party not in breach would suffer if there was a breach of clause B9.1.

C. PAYMENT

C1 Payment and VAT

C1.1 The Supplier shall submit invoices to the Authority in accordance with this clause C1 and Schedule 2.

C1.2 The Authority issues Purchase Orders using Basware and, unless Approved otherwise, the Supplier shall, when invited, register on Basware.

C1.3 If the Supplier registers on Basware, a Valid Invoice is an invoice issued through Basware, unless the invoice contains:

(a) additional lines not included in the relevant Purchase Order;

(b) line descriptions which have been materially altered so that they no longer match the equivalent description in the relevant Purchase Order;

(c) Prices and/or volumes which have been increased without Approval.

C1.4 If, with Approval, the Supplier does not register on Basware, a Valid Invoice is an invoice which includes the information set out in Part 2 of Schedule 2 and, if requested by the Authority:

(a) timesheets for Staff engaged in providing the Services signed and dated by the Authority's representative on the Premises on the day;

(b) the name of the individuals to whom the timesheet relates and hourly rates for each;

(c) identification of which individuals are Supplier's staff and which are Sub-Contractors' staff;

(d) the address of the Premises and the date on which work was undertaken;

(e) the time spent working on the Premises by the individuals concerned;

(f) details of the type of work undertaken by the individuals concerned;

(g) details of plant or materials operated and on standby;

(h) separate identification of time spent travelling and/or meal or rest breaks; and

(i) if appropriate, details of journeys made and distances travelled.

C1.5 The Authority shall not pay an invoice which is not a Valid Invoice.

C1.6 The Authority shall not pay the Supplier's overhead costs unless Approved and overhead costs include, without limitation: facilities, utilities, insurance, tax, head office overheads, indirect staff costs and other costs not specifically and directly ascribable solely to the provision of the Services.

C1.7 If Schedule 2 expressly provides that the Authority may be charged for plant which is on standby then if plant was waiting to be transferred between Premises or if the Authority has instructed that the plant is retained on the Premises then a standby charge of 60% of agreed rates may be made in respect of such relevant periods if supported by timesheets.

C1.8 The Authority shall not pay a stand-by rate if plant is on standby because no work was being carried out on the Premises at that time or no operator or other relevant staff were available (unless the standby is because the Supplier is awaiting licensing of the Premises on the Authority's instructions).

C1.9 The Authority shall not pay for plant or equipment which is stood down during any notice period pursuant to clauses H1, H2 and/or H3 and the Supplier shall mitigate such costs as far as is reasonably possible, for example, by reutilising Staff, plant, materials and services on other contracts.

C1.10 The Supplier may claim expenses only if they are clearly identified, supported by original receipts and Approved.

C1.11 If the Authority pays the Supplier prior to the submission of a Valid Invoice this payment is on account of and deductible from the next payment to be made.

C1.12 If any overpayment has been made or the payment or any part is not supported by a Valid Invoice the Authority may recover this payment against future invoices raised or directly from the Supplier. All payments made by the Authority to the Supplier are on an interim basis pending final resolution of an account with the Supplier in accordance with the terms of this clause C1.

C1.13 The Supplier shall:

(a) add VAT to the Price at the prevailing rate as applicable and show the amount of VAT payable separately on all invoices as an extra charge. If the Supplier fails to show VAT on an invoice, the Authority is not, at any later date, liable to pay the Supplier any additional VAT;

(b) ensure that a provision is included in all Sub-Contracts which requires payment to be made of all sums due to Sub-Contractors within 30 days from the receipt of a valid invoice; and

(c) not suspend the Services unless the Supplier is entitled to terminate the Contract under clause H2.3 for failure to pay undisputed sums of money.

C1.14 The Supplier indemnifies the Authority on a continuing basis against any liability, including any interest, penalties or costs incurred, which is levied, demanded or assessed on the Authority at any time in respect of the Supplier's failure to account for or to pay any VAT relating to payments made to the Supplier under the Contract. Any amounts due under this clause C1.14 shall be paid by the Supplier to the Authority not less than 5 Working Days before the date upon which the tax or other liability is payable by the Authority.

C1.15 The Authority shall:

(a) in addition to the Price and following receipt of a Valid Invoice, pay the Supplier a sum equal to the VAT chargeable on the value of the Services supplied in accordance with the Contract;

(b) pay all sums due to the Supplier within 30 days of receipt of a Valid Invoice unless an alternative arrangement has been Approved.

C1.16 Any late payment of undisputed invoices by the Authority will be subject to interest at the rate of a maximum of 3% above the base rate from time to time of Barclays Bank.

C2 Recovery of Sums Due

C2.1 If under the Contract any sum of money is recoverable from or payable by the Supplier to the Authority (including any sum which the Supplier is liable to pay to the Authority in respect of any breach of the Contract), the Authority may unilaterally deduct that sum from any sum then due, or which at any later time may become due to the Supplier from the Authority under the Contract or under any other agreement with the Authority or the Crown.

C2.2 Any overpayment by either Party, whether of the Price or of VAT or otherwise, is a sum of money recoverable by the Party who made the overpayment from the Party in receipt of the overpayment.

C2.3 The Supplier shall make all payments due to the Authority without any deduction whether by way of set-off, counterclaim, discount, abatement or otherwise unless the Supplier has a valid court order requiring an amount equal to such deduction to be paid by the Authority to the Supplier.

C2.4 All payments due shall be made within a reasonable time unless otherwise specified in the Contract, in cleared funds, to such bank or building society account as the recipient Party may from time to time direct.

C3 Price During Extension

Subject to Schedule 2 and clause F4 (Change), the Price applies for the Initial Term and until the end of any Extension or such earlier date of termination or partial termination of the Contract in accordance with the Law or the Contract.

D. PROTECTION OF INFORMATION

D1 Authority Data

D1.1 The Supplier shall:

(a) not store, copy, disclose, or use the Authority Data except as necessary for the performance by the Supplier of its obligations under the Contract or as otherwise Approved;

(b) preserve the integrity of Authority Data and prevent the corruption or loss of Authority Data;

(c) not delete or remove any proprietary notices contained within or relating to the Authority Data;

(d) to the extent that Authority Data is held and/or processed by the Supplier, supply Authority Data to the Authority as requested by the Authority in the format specified in the Specification;

(e) perform secure back-ups of all Authority Data and ensure that up-to-date back-ups are stored securely off-site. The Supplier shall ensure that such back-ups are made available to the Authority within four hours of request;

(f) ensure that any system on which the Supplier holds any Authority Data, including back-up data, is a secure system that complies with the Security Policy Framework;

(g) identify, and disclose to the Authority on request those members of Staff with access to or who are involved in handling Authority Data;

(h) on request, give the Authority details of its policy for reporting, managing and recovering from information risk incidents, including losses of Personal Data, and its procedures for reducing risk;

(i) notify the Authority immediately and inform the Authority of the remedial action the Supplier proposes to take if it has reason to believe that Authority Data has or may become corrupted, lost or sufficiently degraded in any way for any reason; and

(j) comply with Schedule 6 (Security Requirements and Policy).

D1.2 If Authority Data is corrupted, lost or sufficiently degraded as a result of the Supplier's Default so as to be unusable, the Authority may:

(a) require the Supplier (at the Supplier's cost) to restore or procure the restoration of Authority Data and the Supplier shall do so promptly; and/or

(b) itself restore or procure the restoration of Authority Data, and be repaid by the Supplier any reasonable costs incurred in doing so.

D2 Data Protection and Privacy

D2.1 The Parties acknowledge that for the purposes of Data Protection Legislation:

(a) both Parties are Joint Controllers of Offender Personal Data (to be processed as per Schedule 9 Part A);

(b) the Authority is the Data Controller and the Supplier is the Data Processor of the Authority Data (subject to clause D2.1(c) below), (to be processed as per Schedule 9 Part B); and,

(c) the Supplier is the Data Controller and the Authority is Data Processor of Staff Personal Data (to be processed as per Schedule 9 Part C).

D2.2 The Supplier shall:

(a) notify the Authority immediately if it considers any Authority instructions infringe the Data Protection Legislation;

(b) at its own cost, provide all reasonable assistance to the Authority in the preparation of any Data Protection Impact Assessment prior to starting any processing. Such assistance may, at the Authority's discretion, include:

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

ii) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

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

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

(c) in relation to any Personal Data processed in connection with its obligations under the Contract:

i) process that Personal Data only in accordance with Schedule 9 unless the Supplier is required to do otherwise by Law. If it is so required the Supplier shall promptly notify the Authority before processing the Personal Data unless prohibited by Law;

ii) ensure that it has in place Protective Measures which are appropriate to protect against a Data Loss Event having taken account of the nature of the data to be protected, harm that might result from a Data Loss Event, the state of technological development and the cost of implementing any measures

(d) ensure that:

i) Staff do not process Personal Data except in accordance with the Contract (and in particular Schedule 9;

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

A) are aware of and comply with the Supplier's duties under this clause D2;

B) are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;

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 Authority or as permitted by the Contract;

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

(e) not transfer Personal Data outside the EU unless Approved and:

i) the Authority or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or s.75 of the DPA) as determined by the Authority;

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

iii) the Supplier 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 Authority in meeting its obligations); and

iv) the Supplier complies with any reasonable instructions notified to it in advance by the Authority with respect to the processing of the Personal Data

(f) at the written direction of the Authority, delete or return Personal Data (and any copies of it) to the Authority on termination of the Contract unless the Supplier is required by Law to retain the Personal Data;

(g) subject to clause D2.3, notify the Authority immediately (via email to t: data.compliance@justice.gov.uk and Approvedpremises@justice.gov.uk) if i

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

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

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

iv) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under the Contract;

v) 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

vi) becomes aware of a Data Loss Event.

D2.3 The Supplier's obligation to notify under clause D2.2 (g) includes the provision of further information to the Authority in phases as details become available.

D2.4 Taking into account the nature of the processing, the Supplier shall provide the Authority with full assistance in relation to either Party's obligations under the Data Protection Legislation and any complaint, communication or request made under clause D2.2 (g) (and insofar as possible within the timescales reasonably required by the Authority) including by promptly providing:

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

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

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

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

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

D2.5 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this clause D2. This requirement does not apply if the Supplier employs fewer than 250 people unless the Authority determines that the processing:

(a) is not occasional;

(b) 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; and

(c) is likely to result in a risk to the rights and freedoms of Data Subjects.

D2.6 The Supplier shall allow audits of its Data Processing activity by the Authority or the Authority's designated auditor.

D2.7 The Supplier shall designate a Data Protection Officer if required by the Data Protection Legislation.

D2.8 Before allowing any Sub-processor to process any Personal Data in connection with the Contract, the Supplier shall:

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

(b) obtain Approval;

(c) enter into a written agreement with the Sub-processor which gives effect to the terms set out in this clause D2 such that they apply to the Sub-processor; and

(d) provide the Authority with such information regarding the Sub-processor as the Authority reasonably requires.

D2.9 The Supplier remains fully liable for the acts and omissions of any Sub-processor.

D2.10 Notwithstanding the provisions of clause F4, the Authority may, at any time on not less than 30 Working Days' notice, revise this clause D2 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 the Contract).

D2.11 The Parties shall take account of any guidance published by the Information Commissioner's Office and, notwithstanding the provisions of clause F4, the Authority may on not less than 30 Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance published by the Information Commissioner's Office.

D2.12 In relation to Personal Data processed for Law Enforcement Purposes, the Supplier shall:

(a) maintain logs for its automated processing operations in respect of:

i) collection;

ii) alteration;

iii) consultation;

iv) disclosure (including transfers);

v) combination; and

vi) erasure.

(together the "**Logs**").

(b) ensure that:

i) the Logs of consultation make it possible to establish the justification for, and date and time of, the consultation; and as far as possible, the identity of the person who consulted the data;

ii) the Logs of disclosure make it possible to establish the justification for, and date and time of, the disclosure; and the identity of the recipients of the data; and

iii) the Logs are made available to the Information Commissioner's Office on request

(c) use the Logs only to:

i) verify the lawfulness of processing;

ii) assist with self-monitoring by the Authority or (as the case may be) the Supplier, including the conduct of internal disciplinary proceedings;

iii) ensure the integrity of Personal Data; and

iv) assist with criminal proceedings

(d) as far as possible, distinguish between Personal Data based on fact and Personal Data based on personal assessments; and

(e) where relevant and as far as possible, maintain a clear distinction between Personal Data relating to different categories of Data Subject, for example:

i) persons suspected of having committed or being about to commit a criminal offence;

ii) persons convicted of a criminal offence;

iii) persons who are or maybe victims of a criminal offence; and

iv) witnesses or other persons with information about offences.

D2.13 This clause D2 applies during the Term and indefinitely after its expiry.

D3 Official Secrets Acts and Finance Act

D3.1 The Supplier shall comply with:

(a) the Official Secrets Acts 1911 to 1989; and

(b) section 182 of the Finance Act 1989.

D4 Confidential Information

D4.1 Except to the extent set out in this clause D4 or if disclosure or publication is expressly allowed elsewhere in the Contract each Party shall treat all Confidential Information belonging to the other Party as confidential and shall not disclose any Confidential Information belonging to the other Party to any other person without the other Party's consent, except to such persons and to such extent as may be necessary for the performance of the Party's obligations under the Contract.

D4.2 The Supplier hereby gives its consent for the Authority to publish the whole Contract (but with any information which is Confidential Information belonging to the Authority redacted) including from time to time agreed changes to the Contract, to the general public.

D4.3 If required by the Authority, the Supplier shall ensure that Staff, professional advisors and consultants sign a non-disclosure agreement prior to commencing any work in connection with the Contract in a form approved by the Authority. The Supplier shall maintain a list of the non-disclosure agreements completed in accordance with this clause D4.3.

D4.4 If requested by the Authority, the Supplier shall give the Authority a copy of the list and, subsequently upon request by the Authority, copies of such of the listed non-disclosure agreements as required by the Authority. The Supplier shall ensure that Staff, professional advisors and consultants are aware of the Supplier's confidentiality obligations under the Contract.

D4.5 The Supplier may disclose the Authority's Confidential Information only to Staff who are directly involved in providing the Services and who need to know the information, and shall ensure that such Staff are aware of and shall comply with these obligations as to confidentiality.

D4.6 The Supplier shall not, and shall procure that the Staff do not, use any of the Authority's Confidential Information received otherwise than for the purposes of the Contract.

D4.7 Clause D4.1 shall not apply to the extent that:

(a) such disclosure is a requirement of Law placed upon the Party making the disclosure, including any requirements for disclosure under the FOIA or the EIR;

(b) such information was in the possession of the Party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner;

(c) such information was obtained from a third party without obligation of confidentiality;

(d) such information was already in the public domain at the time of disclosure otherwise than by a breach of the Contract; or

(e) it is independently developed without access to the other Party's Confidential Information.

D4.8 Nothing in clause D4.1 prevents the Authority disclosing any Confidential Information obtained from the Supplier:

(a) for the purpose of the examination and certification of the Authority's accounts;

(b) for the purpose of any examination pursuant to section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority has used its resources;

(c) to Parliament and Parliamentary committees;

(d) to any Crown Body or any Contracting Authority and the Supplier hereby acknowledges that all Government departments or Contracting Authorities receiving such Confidential Information may further disclose the Confidential Information to other Government departments or other Contracting Authorities on the basis that the information is

confidential and is not to be disclosed to a third party which is not part of any Government department or any Contracting Authority; or

(e) to any consultant, contractor or other person engaged by the Authority

provided that in disclosing information under clauses D4.8 (d) and (e) the Authority discloses only the information which is necessary for the purpose concerned and requests that the information is treated in confidence and that a confidentiality undertaking is given where appropriate.

D4.9 Nothing in clauses D4.1 to D4.6 prevents either Party from using any techniques, ideas or Know-How gained during the performance of its obligations under the Contract in the course of its normal business, to the extent that this does not result in a disclosure of the other Party's Confidential Information or an infringement of the other Party's Intellectual Property Rights.

D4.10 The Authority shall use reasonable endeavours to ensure that any Government department, Contracting Authority, employee, third party or Sub-Contractor to whom the Supplier's Confidential Information is disclosed pursuant to clause D4.8 is made aware of the Authority's obligations of confidentiality.

D4.11 If the Supplier does not comply with clauses D4.1 to D4.8 the Authority may terminate the Contract immediately on notice.

D4.12 To ensure that no unauthorised person gains access to any Confidential Information or any data obtained in the supply of the Services, the Supplier shall maintain adequate security arrangements that meet the requirements of professional standards and best practice.

D4.13 The Supplier shall:

(a) immediately notify the Authority of any breach of security in relation to Confidential Information and all data obtained in the supply of the Services and will keep a record of such breaches;

(b) use best endeavours to recover such Confidential Information or data however it may be recorded;

(c) co-operate with the Authority in any investigation as a result of any breach of security in relation to Confidential Information or data; and

(d) at its own expense, alter any security systems at any time during the Term at the Authority's request if the Authority reasonably believes the Supplier has failed to comply with clause D4.12.

D5 Freedom of Information

D5.1 The Supplier acknowledges that the Authority is subject to the requirements of the FOIA and the EIR.

D5.2 The Supplier shall:

(a) transfer to the Authority all Requests for Information that it receives as soon as practicable and in any event within a maximum of 2 Working Days of receipt;

(b) give the Authority a copy of all Information in its possession or control in the form that the Authority requires within 5 Working Days (or such other period as the Authority may specify) of the Authority's request;

(c) provide all necessary assistance as reasonably requested by the Authority to enable the Authority to comply with its obligations under the FOIA and EIR; and

(d) not respond directly to a Request for Information unless authorised to do so in writing by the Authority.

D5.3 The Authority shall determine in its absolute discretion and notwithstanding any other provision in the Contract or any other agreement whether the Commercially Sensitive Information and any other Information is exempt from disclosure in accordance with the FOIA and/or the EIR.

D6 Publicity, Media and Official Enquiries

D6.1 The Supplier shall not:

(a) make any press announcements or publicise the Contract or its contents in any way;

(b) use the Authority's name, brand or logo in any publicity, promotion, marketing or announcement of order; or

(c) use the name, brand or logo of any of the Authority's agencies or arms-length bodies in any publicity, promotion, marketing or announcement of orders

without Approval.

D6.2 Each Party acknowledges that nothing in the Contract either expressly or impliedly constitutes an endorsement of any products or services of the other Party (including the Services and the ICT Environment) and each Party shall not conduct itself in such a way as to imply or express any such approval or endorsement.

D6.3 The Supplier shall use reasonable endeavours to ensure that its Staff and professional advisors comply with clause D6.1.

E. INTELLECTUAL PROPERTY

E1 Intellectual Property Rights

E1.1 All Intellectual Property Rights in:

(a) the Results; or

(b) any guidance, specifications, reports, studies, instructions, toolkits, plans, data, drawings, databases, patents, patterns, models, designs or other material which is furnished to or made available to the Supplier by or on behalf of the Authority (together with the Results, the "**IP Materials**") shall vest in the Authority (save for Copyright and Database Rights which shall vest in Her Majesty the Queen) and the Supplier shall not, and shall ensure that the Staff shall not, use or disclose any IP Materials without Approval save to the extent necessary for performance by the Supplier of its obligations under the Contract.

E1.2 The Supplier hereby assigns:

(a) to the Authority, with full title guarantee, all Intellectual Property Rights (save for Copyright and Database Rights) which may subsist in the IP Materials. This assignment shall take effect on the date of the Contract or (in the case of rights arising after the date of the Contract) as a present assignment of future rights that will take effect immediately on the coming into existence of the Intellectual Property Rights produced by the Supplier; and

(b) to Her Majesty the Queen, with full title guarantee, all Copyright and Database Rights which may subsist in the IP Materials

and shall execute all documents and do all acts as are necessary to execute these assignments.

E1.3 The Supplier shall:

(a) waive or procure a waiver of any moral rights held by it or any third party in copyright material arising as a result of the Contract or the performance of its obligations under the Contract;

(b) ensure that the third-party owner of any Intellectual Property Rights that are or which may be used to perform the Services grants to the Authority a non-exclusive licence or, if itself a licensee of those rights, shall grant to the Authority an authorised sub-licence, to use, reproduce, modify, develop and maintain the Intellectual Property Rights in the same. Such licence or sub-licence shall be non-exclusive, perpetual, royalty-free, worldwide and irrevocable and include the right for the Authority to sub-license, transfer, novate or assign to other Contracting Authorities, the Crown, the Replacement Supplier or to any other third party supplying goods and/or services to the Authority ("**Indemnified Persons**");

(c) not infringe any Intellectual Property Rights of any third party in supplying the Services; and

(d) during and after the Term, indemnify and keep indemnified the Authority and Indemnified Persons from and against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and other liabilities which the Authority and Indemnified Persons may suffer or incur as a result of or in connection with any breach of this clause E1.3, except to the extent that any such claim results directly from:

i) items or materials based upon designs supplied by the Authority; or

ii) the use of data supplied by the Authority which is not required to be verified by the Supplier under any provision of the Contract.

E1.4 The Authority shall notify the Supplier in writing of any claim or demand brought against the Authority or Indemnified Person for infringement or alleged infringement of any Intellectual Property Right in materials supplied and/or licensed by the Supplier to the Authority.

E1.5 The Supplier shall at its own expense conduct all negotiations and any litigation arising in connection with any claim, demand or action by any third party for infringement or alleged infringement of any third party Intellectual Property Rights (whether by the Authority, the Supplier or Indemnified Person) arising from the performance of the Supplier's obligations under the Contract ("**Third Party IP Claim**"), provided that the Supplier shall at all times:

(a) consult the Authority on all material issues which arise during the conduct of such litigation and negotiations;

(b) take due and proper account of the interests of the Authority; and

(c) not settle or compromise any claim without Approval (not to be unreasonably withheld or delayed).

E1.6 The Authority shall, at the request of the Supplier, afford to the Supplier all reasonable assistance for the purpose of contesting any Third-Party IP Claim and the Supplier shall indemnify the Authority for all costs and expenses (including, but not limited to, legal costs and disbursements) incurred in doing so. The Supplier is not required to indemnify the Authority under this clause E1 in relation to any costs and expenses to the extent that such arise directly from the matters referred to in clauses E1.3 (d) i) and ii).

E1.7 The Authority shall not, without the Supplier's consent, make any admissions which may be prejudicial to the defence or settlement of any Third-Party IP Claim.

E1.8 If any Third-Party IP Claim is made or in the reasonable opinion of the Supplier is likely to be made, the Supplier shall notify the Authority and any relevant Indemnified Person, at its own expense and subject to Approval (not to be unreasonably withheld or delayed), shall (without prejudice to the rights of the Authority under clauses E1.3 (b) and G2.1 (g)) use its best endeavours to:

(a) modify any or all of the Services without reducing the performance or functionality of the same, or substitute alternative services of equivalent performance and functionality, so as to avoid the infringement or the alleged infringement; or

(b) procure a licence to use the Intellectual Property Rights and supply the Services which are the subject of the alleged infringement, on terms which are acceptable to the Authority

and if the Supplier is unable to comply with clauses E1.8 (a) or (b) within 20 Working Days of receipt by the Authority of the Supplier's notification the Authority may terminate the Contract immediately by notice to the Supplier.

E1.9 The Supplier grants to the Authority and, if requested by the Authority, to a Replacement Supplier, a royalty-free, irrevocable, worldwide, non-exclusive licence (with a right to sub-license) to use any Intellectual Property Rights that the Supplier owned or developed prior to the Commencement Date and which the Authority (or the Replacement Supplier) reasonably requires in order for the Authority to exercise its rights under, and receive the benefit of, the Contract (including, without limitation, the Services).

F. CONTROL OF THE CONTRACT

F1 Contract Performance

F1.1 The Supplier shall immediately inform the Authority if any of the Services are not being or are unable to be performed, the reasons for non-performance, any corrective action and the date by which that action will be completed.

F1.2 At or around 6 Months from the Commencement Date and each anniversary of the Commencement Date thereafter, the Authority may carry out a review of the performance of the Supplier (a "**Review**"). Without prejudice to the generality of the foregoing, the Authority may in respect of the period under review consider such items as (but not limited to):

a) the Supplier's delivery of the Services;

b) the Supplier's contribution to innovation in the Authority; whether the Services provide the Authority with best value for money; consideration of any changes which may need to be made to the Services;

c) a review of future requirements in relation to the Services; and

d) progress against key milestones.

F1.3 The Supplier shall provide at its own cost any assistance reasonably required by the Authority to perform Reviews including the provision of data and information.

F1.4 The Authority may produce a report (a "**Review Report**") of the results of each Review stating any areas of exceptional performance and areas for improvement in the provision of the Services and where there is any shortfall in any aspect of performance reviewed as against the Authority's expectations and the Supplier's obligations under the Contract.

F1.5 The Authority shall give the Supplier a copy of the Review Report (if applicable). The Authority shall consider any Supplier comments and may produce a revised Review Report.

F1.6 The Supplier shall, within 10 Working Days of receipt of the Review Report (revised as appropriate) provide the Authority with a plan to address resolution of any shortcomings and implementation of improvements identified by the Review Report.

F1.7 Actions required to resolve shortcomings and implement improvements (either as a consequence of the Supplier's failure to meet its obligations under the Contract identified by the Review Report, or those which result from the Supplier's failure to meet the Authority's expectations notified to the Supplier or of which the Supplier ought reasonably to have been aware) shall be implemented at no extra cost to the Authority.

F2 Remedies

F2.1 If the Authority reasonably believes the Supplier has committed a Material Breach it may, without prejudice to its rights under clause H2 (Termination on Default), do any of the following:

(a) without terminating the Contract, itself supply or procure the supply of all or part of the Services until such time as the Supplier has demonstrated to the Authority's reasonable

satisfaction that the Supplier will be able to supply the Services in accordance with the Specification;

(b) without terminating the whole of the Contract, terminate the Contract in respect of part of the Services only (whereupon a corresponding reduction in the Price shall be made) and thereafter itself supply or procure a third party to supply such part of the Services;

(c) withhold or reduce payments to the Supplier in such amount as the Authority reasonably deems appropriate in each particular case; and/or

(d) terminate the Contract in accordance with clause H2.

F2.2 Without prejudice to its right under clause C3 (Recovery of Sums Due), the Authority may charge the Supplier for any costs reasonably incurred and any reasonable administration costs in respect of the supply of any part of the Services by the Authority or a third party to the extent that such costs exceed the payment which would otherwise have been payable to the Supplier for such part of the Services.

F2.3 If the Authority reasonably believes the Supplier has failed to supply all or any part of the Services in accordance with the Contract, professional or Good Industry Practice which could reasonably be expected of a competent and suitably qualified person, or any legislative or regulatory requirement, the Authority may give the Supplier notice specifying the way in which its performance falls short of the requirements of the Contract or is otherwise unsatisfactory.

F2.4 If the Supplier has been notified of a failure in accordance with clause F2.3 the Authority may:

(a) direct the Supplier to identify and remedy the failure within such time as may be specified by the Authority and to apply all such additional resources as are necessary to remedy that failure at no additional charge to the Authority within the specified timescale; and/or

(b) withhold or reduce payments to the Supplier in such amount as the Authority deems appropriate in each particular case until such failure has been remedied to the satisfaction of the Authority.

F2.5 If the Supplier has been notified of a failure in accordance with clause F2.3, it shall:

(a) use all reasonable endeavours to immediately minimise the impact of such failure to the Authority and to prevent such failure from recurring; and

(b) immediately give the Authority such information as the Authority may request regarding what measures are being taken to comply with the obligations in this clause F2.5 and the progress of those measures until resolved to the satisfaction of the Authority.

F2.6 If, having been notified of any failure, the Supplier does not remedy it in accordance with clause F2.5 in the time specified by the Authority, the Authority may treat the continuing failure as a Material Breach and may terminate the Contract immediately on notice to the Supplier.

F3 Transfer and Sub-Contracting

F3.1 Except where both clauses F3.9 and F3.10 apply, the Supplier shall not transfer, charge, assign, sub-contract or in any other way dispose of the Contract or any part of it without Approval. All such actions shall be evidenced in writing and shown to the Authority on request. Sub-contracting any part of the Contract does not relieve the Supplier of any of its obligations or duties under the Contract.

F3.2 The Supplier is responsible for the acts and/or omissions of its Sub-Contractors as though they are its own. If it is appropriate, the Supplier shall provide each Sub-Contractor with a copy of the Contract and obtain written confirmation from them that they will provide the Services fully in accordance with the Contract.

F3.3 The Supplier shall ensure that Sub-Contractors retain all records relating to the Services for at least 6 years from the date of their creation and make them available to the Authority on request in accordance with clause F5 (Audit). If any Sub-Contractor does not allow the Authority access to the records then the Authority shall have no obligation to pay any claim or invoice made by the Supplier on the basis of such documents or work carried out by the Sub-Contractor.

F3.4 If the Authority has consented to the award of a Sub-Contract, the Supplier shall ensure that:

(a) the Sub-Contract contains:

i) a right for the Supplier to terminate the if the Sub-Contractor does not comply with its legal obligations in connection with Data Protection Legislation, environmental, social or labour law; and

ii) obligations no less onerous on the Sub-Contractor than those on the Supplier under the Contract in respect of data protection in clauses D1 and D2

(b) the Sub-Contractor includes a provision having the same effect as set out in this clause F3.4 (a) in any Sub-Contract which it awards; and

(c) copies of each Sub-Contract are sent to the Authority immediately after their execution.

F3.5 Unless Approved otherwise, if the total value of the Contract over the Term is, or is likely to be, in excess of £5,000,000, the Supplier shall, in respect of Sub-Contract opportunities arising during the Term from or in connection with the provision of the Services:

(a) advertise on Contracts Finder those that have a value in excess of £25,000;

(b) within 90 days of awarding a Sub-Contract, update the notice on Contracts Finder with details of the Sub-Contractor;

(c) monitor the number, type and value of the Sub-Contract opportunities placed on Contracts Finder and awarded during the Term;

(d) provide reports on the information in clause F3.5 (c) to the Authority in the format and frequency reasonably specified by the Authority;

(e) promote Contracts Finder to its suppliers and encourage them to register on Contracts Finder; and

(f) ensure that each advertisement placed pursuant to F3.5 (a) includes a full and detailed description of the Sub-Contract opportunity with each of the mandatory fields being completed on Contracts Finder.

F3.6 The Supplier shall, at its own cost, supply to the Authority by the end of April each year for the previous Financial Year:

(a) the total revenue received from the Authority pursuant to the Contract;

(b) the total value of all its Sub-Contracts;

(c) the total value of its Sub-Contracts with SMEs; and

(d) the total value of its Sub-Contracts with VCSEs.

F3.7 The Authority may from time to time change the format and the content of the information required pursuant to clause F3.6.

F3.8 If the Authority believes there are:

(a) compulsory grounds for excluding a Sub-Contractor pursuant to regulation 57 of the Regulations, the Supplier shall replace or not appoint the Sub-Contractor; or

(b) non-compulsory grounds for excluding a Sub-Contractor pursuant to regulation 57 of the Regulations, the Authority may require the Supplier to replace or not appoint the Sub-Contractor and the Supplier shall comply with such requirement.

F3.9 Notwithstanding clause F3.1, the Supplier may assign to a third party (the "**Assignee**") the right to receive payment of the Price or any part thereof due to the Supplier (including any interest which the Authority incurs under clause C1 (Payment and VAT)). Any assignment under this clause F3.9 is subject to:

(a) reduction of any sums in respect of which the Authority exercises its right of recovery under clause C2 (Recovery of Sums Due);

(b) all related rights of the Authority under the Contract in relation to the recovery of sums due but unpaid; and

(c) the Authority receiving notification under both clauses F3.10 and F3.11.

F3.10 If the Supplier assigns the right to receive the Price under clause F3.9, the Supplier or the Assignee shall notify the Authority in writing of the assignment and the date upon which the assignment becomes effective.

F3.11 The Supplier shall ensure that the Assignee notifies the Authority of the Assignee's contact information and bank account details to which the Authority can make payment.

F3.12 Clause C1 continues to apply in all other respects after the assignment and shall not be amended without Approval.

F3.13 Subject to clause F3.14, the Authority may assign, novate or otherwise dispose of its rights and obligations under the Contract or any part thereof to:

(a) any Contracting Authority;

(b) any other body established or authorised by the Crown or under statute in order substantially to perform any of the functions that had previously been performed by the Authority; or

(c) any private sector body which substantially performs the functions of the Authority

provided that any such assignment, novation or other disposal shall not increase the burden of the Supplier's obligations under the Contract.

F3.14 Any change in the legal status of the Authority such that it ceases to be a Contracting Authority shall not, subject to clause F3.15, affect the validity of the Contract and the Contract shall bind and inure to the benefit of any successor body to the Authority.

F3.15 If the rights and obligations under the Contract are assigned, novated or otherwise disposed of pursuant to clause F3.13 to a body which is not a Contracting Authority or if there is a change in the legal status of the Authority such that it ceases to be a Contracting Authority (in the remainder of this clause both such bodies being referred to as the **"Transferee"**):

(a) the rights of termination of the Authority in clauses H1 and H2 are available to the Supplier in respect of the Transferee; and

(b) the Transferee shall only be able to assign, novate or otherwise dispose of its rights and obligations under the Contract or any part thereof with the prior consent in writing of the Supplier.

F3.16 The Authority may disclose to any Transferee any Confidential Information of the Supplier which relates to the performance of the Supplier's obligations under the Contract. In such circumstances the Authority shall authorise the Transferee to use such Confidential Information only for purposes relating to the performance of the Supplier's obligations under the Contract and for no other purpose and shall take all reasonable steps to ensure that the Transferee gives a confidentiality undertaking in relation to such Confidential Information.

F3.17 Each Party shall at its own cost and expense carry out, or use all reasonable endeavours to ensure the carrying out of, whatever further actions (including the execution of further documents) the other Party reasonably requires from time to time for the purpose of giving that other Party the full benefit of the Contract.

F4 Change

F4.1 After the Commencement Date, either Party may request a Change subject to the terms of this clause F4.

F4.2 Either Party may request a Change by notifying the other Party in writing of the Change by completing the Change Request Form set out in Schedule 3. The Party requesting the Change shall give the other Party sufficient information and time to assess the extent and effect of the

requested Change. If the receiving Party accepts the Change it shall confirm it in writing to the other Party.

F4.3 If the Supplier is unable to accept a Change requested by the Authority or if the Parties are unable to agree a change to the Price, the Authority may:

(a) allow the Supplier to fulfil its obligations under the Contract without the Change; or

(b) terminate the Contract immediately except where the Supplier has already delivered all or part of the Services or where the Supplier can show evidence of substantial work being carried out to fulfil the requirements of the Specification; and in such case the Parties shall attempt to agree upon a resolution to the matter. If a resolution cannot be reached, the matter shall be dealt with under the Dispute Resolution procedure detailed in clause I2 (Dispute Resolution).

F4.4 A Change takes effect only when it is recorded in a CCN validly executed by both Parties.

F4.5 The Supplier is deemed to warrant and represent that the CNN has been executed by a duly authorised representative of the Supplier in addition to the warranties and representations set out in clause G2.

F4.6 Clauses F4.4 and F4.5 may be varied in an emergency if it is not practicable to obtain the Authorised Representative's approval within the time necessary to make the Change in order to address the emergency. In an emergency, Changes may be approved by a different representative of the Authority. However, the Authorised Representative may review such a Change and require a CCN to be entered into on a retrospective basis which may itself vary the emergency Change.

F5 Audit

F5.1 The Supplier shall:

(a) keep and maintain until 6 years after the end of the Term, or as long a period as may be agreed between the Parties, full and accurate records of the Contract including the Services supplied under it, all expenditure reimbursed by the Authority, and all payments made by the Authority;

(b) on request afford the Authority or the Authority's representatives such access to those records and processes as may be requested by the Authority in connection with the Contract;

(c) make available to the Authority, free of charge, whenever requested, copies of audit reports obtained by the Supplier in relation to the Services;

(d) allow authorised representatives of the Authority and/or the National Audit Office to examine the Supplier's records and documents relating to the Contract and provide such copies and oral or written explanations as may reasonably be required; and

(e) allow the Comptroller and Auditor General (and his appointed representatives) access free of charge during normal business hours on reasonable notice to all such documents (including computerised documents and data) and other information as the Comptroller and Auditor General may reasonably require for the purposes of his

financial audit of the Authority and for carrying out examinations into the economy, efficiency and effectiveness with which the Authority has used its resources. The Supplier shall provide such explanations as are reasonably required for these purposes.

F5.2 The Authority, acting by itself or through its duly authorised representatives and/or the National Audit Office, may, during the Term and for a period of 18 Months thereafter, assess compliance by the Supplier of the Supplier's obligations under the Contract, including to:

(a) verify the accuracy of the Price and any other amounts payable by the Authority under the Contract;

(b) verify the Open Book Data;

(c) verify the Supplier's compliance with the Contract and applicable Law;

(d) identify or investigate actual or suspected fraud, impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Authority has no obligation to inform the Supplier of the purpose or objective of its investigations;

(e) identify or investigate any circumstances which may impact upon the financial stability of the Supplier and/or any guarantor or their ability to perform the Services;

(f) obtain such information as is necessary to fulfil the Authority's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes;

(g) carry out the Authority's internal and statutory audits and to prepare, examine and/or certify the Authority's annual and interim reports and accounts;

(h) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority has used its resources;

(i) verify the accuracy and completeness of any management information or reports delivered or required by the Contract;

(j) review the Supplier's compliance with the Authority's policies and standards; and/or

(k) review the integrity, confidentiality and security of the Authority Data

and the Supplier (and its agents) shall permit access free of charge during normal business hours on reasonable notice to all such documents (including computerised documents and data) and other information as the Authority (or those acting on its behalf) may reasonably require for the purposes of conducting such an audit.

F5.3 The Authority shall during each audit comply with those security, sites, systems and facilities operating procedures of the Supplier that the Authority deems reasonable and use its reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Supplier or delay the provision of the Services. The Authority shall endeavour to

(but is not obliged to) provide at least 15 Working Days' notice of its intention to conduct an audit.

F5.4 The Parties bear their own respective costs and expenses incurred in respect of compliance with their obligations under clause F5, unless the audit identifies a material Default by the Supplier in which case the Supplier shall reimburse the Authority for all the Authority's reasonable costs incurred in connection with the audit.

G. LIABILITIES

G1 Liability, Indemnity and Insurance

G1.1 Neither Party limits its liability for:

(a) death or personal injury caused by its negligence;

(b) fraud or fraudulent misrepresentation;

(c) any breach of any obligations implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Goods and Services Act 1982;

(d) any breach of clauses D1, D2 or D4 or Schedules 6 or 8; or

(e) any liability to the extent it cannot be limited or excluded by Law.

G1.2 Subject to clauses G1.3 and G1.5, the Supplier indemnifies the Authority fully against all claims, proceedings, demands, charges, actions, damages, costs, breach of statutory duty, expenses and any other liabilities which may arise out of the supply, or the late or purported supply, of the Services or the performance or non-performance by the Supplier of its obligations under the Contract or the presence of the Supplier or any Staff on the Premises, including in respect of any death or personal injury, loss of or damage to property, financial loss arising from any advice given or omitted to be given by the Supplier, or any other loss which is caused directly by any act or omission of the Supplier.

G1.3 From the second year of the Contract and subject to clause G1.1, the Supplier's aggregate liability in respect of the Contract does not exceed the Price payable in the previous calendar year of the Contract. For the first year of the Contract, the Supplier's aggregate liability in respect of the Contract does not exceed the Price payable in the final calendar year of the previous contract for the Services.

G1.4 From the second year of the Contract and subject to clause G1.1 the Authority's aggregate liability in respect of the Contract does not exceed the Price payable in the previous calendar year of the Contract. For the first year of the Contract, the Authority's aggregate liability in respect of the Contract does not exceed the Price payable in the final calendar year of the previous contract for the Services.

G1.5 The Supplier is not responsible for any injury, loss, damage, cost or expense if and to the extent that it is caused by the negligence or wilful misconduct of the Authority or by breach by the Authority of its obligations under the Contract.

G1.6 The Authority may recover from the Supplier the following losses incurred by the Authority to the extent they arise as a result of a Default by the Supplier:

(a) any additional operational and/or administrative costs and expenses incurred by the Authority, including costs relating to time spent by or on behalf of the Authority in dealing with the consequences of the Default;

(b) any wasted expenditure or charges;

(c) the additional costs of procuring a Replacement Supplier for the remainder of the Term and or replacement deliverables which shall include any incremental costs associated with the Replacement Supplier and/or replacement deliverables above those which would have been payable under the Contract;

(d) any compensation or interest paid to a third party by the Authority; and

(e) any fine or penalty incurred by the Authority pursuant to Law and any costs incurred by the Authority in defending any proceedings which result in such fine or penalty.

G1.7 Subject to clauses G1.1 and G1.6, neither Party is liable to the other for any:

(a) loss of profits, turnover, business opportunities or damage to goodwill; or

(b) indirect, special or consequential loss.

G1.8 Unless otherwise specified by the Authority, the Supplier shall, with effect from the Commencement Date for such period as necessary to enable the Supplier to comply with its obligations herein, take out and maintain with a reputable insurance company a policy or policies of insurance providing an adequate level of cover in respect of all risks which may be incurred by the Supplier, arising out of the Supplier's performance of its obligations under the Contract including:

(a) if required by the Authority, appropriate, professional indemnity insurance in the sum of not less than £5,000,000 (five million pounds) for any advice given by the Supplier to the Authority;

(b) cover for death or personal injury, loss of or damage to property or any other loss; and

(c) employer's liability insurance in respect of Staff.

Such insurance policies shall be maintained for the duration of the Term and for a minimum of 6 years following the end of the Term.

G1.9 The Supplier shall give the Authority, on request, copies of all insurance policies referred to in this clause or a broker's verification of insurance to demonstrate that the appropriate cover is in place, together with receipts or other evidence of payment of the latest premiums due under those policies.

G1.10 If the Supplier does not have and maintain the insurances required by the Contract, the Authority may make alternative arrangements to protect its interests and may recover the costs of such arrangements from the Supplier.

G1.11 The provisions of any insurance or the amount of cover shall not relieve the Supplier of any liabilities under the Contract.

G1.12 The Supplier shall not take any action or fail to take any reasonable action, or (to the extent that it is reasonably within its power) permit anything to occur in relation to the Supplier, which would entitle any insurer to refuse to pay any claim under any insurance policy in which the Supplier is an insured, a co-insured or additional insured person.

G2 Warranties and Representations

G2.1 The Supplier warrants and represents on the Commencement Date and for the Term that:

(a) it has full capacity and authority and all necessary consents to enter into and perform the Contract and that the Contract is executed by a duly authorised representative of the Supplier;

(b) in entering the Contract, it has not committed any fraud;

(c) as at the Commencement Date, all information contained in the Tender or other offer made by the Supplier to the Authority remains true, accurate and not misleading, save as may have been specifically disclosed in writing to the Authority prior to execution of the Contract and in addition, that it will advise the Authority of any fact, matter or circumstance of which it may become aware which would render such information to be false or misleading;

(d) no claim is being asserted and no litigation, arbitration or administrative proceeding is in progress or, to the best of its knowledge and belief, pending or threatened against it or any of its assets which will or might have an adverse effect on its ability to perform its obligations under the Contract;

(e) it is not subject to any contractual obligation, compliance with which is likely to have a material adverse effect on its ability to perform its obligations under the Contract;

(f) no proceedings or other steps have been taken and not discharged (or, to the best of its knowledge, are threatened) for the winding up of the Supplier or for its dissolution or for the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Supplier's assets or revenue;

(g) it owns, or has obtained or is able to obtain valid licences for, all Intellectual Property Rights that are necessary for the performance of its obligations under the Contract;

(h) any person engaged by the Supplier shall be engaged on terms which do not entitle them to any Intellectual Property Right in any IP Materials;

(i) in the 3 years (or period of existence if the Supplier has not been in existence for 3 years) prior to the date of the Contract:

i) it has conducted all financial accounting and reporting activities in compliance in all material respects with the generally accepted accounting principles that apply to it in any country where it files accounts;

ii) it has been in full compliance with all applicable securities and tax laws and regulations in the jurisdiction in which it is established; and

iii) it has not done or omitted to do anything which could have a material adverse effect on its assets, financial condition or position as an ongoing business concern or its ability to fulfil its obligations under the Contract;

(j) it has and will continue to hold all necessary (if any) regulatory approvals from the Regulatory Bodies necessary to perform its obligations under the Contract; and

(k) it has notified the Authority in writing of any Occasions of Tax Non-Compliance and any litigation in which it is involved that is in connection with any Occasion of Tax Non-Compliance.

G2.2 The Supplier confirms that in entering into the Contract it is not relying on any statements, warranties or representations given or made (whether negligently or innocently or whether express or implied), or any acts or omissions by or on behalf of the Authority in connection with the subject matter of the Contract except those expressly set out in the Contract and the Supplier hereby waives and releases the Authority in respect thereof absolutely.

G3 Tax Compliance

G3.1 If, during the Term, an Occasion of Tax Non-Compliance occurs, the Supplier shall:

(a) notify the Authority in writing of such fact within 5 Working Days of its occurrence; and

(b) promptly give the Authority:

i) details of the steps it is taking to address the Occasion of Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors it considers relevant; and

ii) such other information in relation to the Occasion of Tax Non-Compliance as the Authority may reasonably require.

G3.2 If the Supplier or any Staff are liable to be taxed in the UK or to pay NICs in respect of consideration received under the Contract, the Supplier shall:

(a) at all times comply with ITEPA and all other statutes and regulations relating to income tax, and SSCBA and all other statutes and regulations relating to NICs, in respect of that consideration; and

(b) indemnify the Authority against any income tax, NICs and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made in connection with the provision of the Services by the Supplier or any Staff.

H. DEFAULT, DISRUPTION AND TERMINATION

H1 Insolvency and Change of Control

H1.1 The Authority may terminate the Contract with immediate effect by notice and without compensation to the Supplier if the Supplier is a company and in respect of the Supplier:

(a) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors;

(b) a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation);

(c) a petition is presented for its winding up (which is not dismissed within 14 days of its service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting is convened pursuant to section 98 of the Insolvency Act 1986;

(d) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets;

(e) an application order is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given;

(f) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986;

(g) being a "small company" within the meaning of section 247(3) of the Companies Act 1985, a moratorium comes into force pursuant to Schedule A1 of the Insolvency Act 1986; or

(h) any event similar to those listed in H1.1 (a)-(g) occurs under the law of any other jurisdiction.

H1.2 The Authority may terminate the Contract with immediate effect by notice and without compensation to the Supplier if the Supplier is an individual and:

(a) an application for an interim order is made pursuant to sections 252-253 of the Insolvency Act 1986 or a proposal is made for any composition scheme or arrangement with, or assignment for the benefit of, the Supplier's creditors;

(b) a petition is presented and not dismissed within 14 days or order made for the Supplier's bankruptcy;

(c) a receiver, or similar officer is appointed over the whole or any part of the Supplier's assets or a person becomes entitled to appoint a receiver, or similar officer over the whole or any part of his assets;

(d) he is unable to pay his debts or has no reasonable prospect of doing so, in either case within the meaning of section 268 of the Insolvency Act 1986;

(e) a creditor or encumbrancer attaches or takes possession of, or a distress, execution, sequestration or other such process is levied or enforced on or sued against, the whole or any part of the Supplier's assets and such attachment or process is not discharged within 14 days;

(f) he dies or is adjudged incapable of managing his affairs within the meaning of section 2 of the Mental Capacity Act 2005;

(g) he suspends or ceases, or threatens to suspend or cease, to carry on all or a substantial part of his business; or

(h) any event similar to those listed in clauses H1.2(a) to (g) occurs under the law of any other jurisdiction.

H1.3 The Supplier shall notify the Authority immediately following a merger, take-over, change of control, change of name or status including where the Supplier undergoes a change of control within the meaning of section 1124 of the Corporation Taxes Act 2010 (**"Change of Control"**). The Authority may terminate the Contract with immediate effect by notice and without compensation to the Supplier within 6 Months of:

(a) being notified that a Change of Control has occurred; or

(b) where no notification has been made, the date that the Authority becomes aware of the Change of Control

but is not permitted to terminate where Approval was granted prior to the Change of Control.

H1.4 The Authority may terminate the Contract with immediate effect by notice and without compensation to the Supplier if the Supplier is a partnership and:

(a) a proposal is made for a voluntary arrangement within Article 4 of the Insolvent Partnerships Order 1994 or a proposal is made for any other composition, scheme or arrangement with, or assignment for the benefit of, its creditors; or

(b) a petition is presented for its winding up or for the making of any administration order, or an application is made for the appointment of a provisional liquidator; or

(c) a receiver, or similar officer is appointed over the whole or any part of its assets; or

(d) the partnership is deemed unable to pay its debts within the meaning of section 222 or 223 of the Insolvency Act 1986 as applied and modified by the Insolvent Partnerships Order 1994; or

(e) any of the following occurs in relation to any of its partners:

(i) an application for an interim order is made pursuant to sections 252-253 of the Insolvency Act 1986 or a proposal is made for any composition scheme or arrangement with, or assignment for the benefit of, his creditors;
(ii) a petition is presented for his bankruptcy; or

(iii) a receiver, or similar officer is appointed over the whole or any part of his assets;

(f) any event similar to those listed in clauses H1.4 (a) to (e) occurs under the law of any other jurisdiction.

H1.5 The Authority may terminate the Contract with immediate effect by notice and without compensation to the Supplier if the Supplier is a limited liability partnership and:

(a) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or a proposal is made for any other composition, scheme or arrangement with, or assignment for the benefit of, its creditors;

(b) an application is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given within Part II of the Insolvency Act 1986;

(c) any step is taken with a view to it being determined that it be wound up (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation) within Part IV of the Insolvency Act 1986;

(d) a petition is presented for its winding up (which is not dismissed within 14 days of its service) or an application is made for the appointment of a provisional liquidator within Part IV of the Insolvency Act 1986;

(e) a receiver, or similar officer is appointed over the whole or any part of its assets; or

(f) it is or becomes unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986;

(g) a moratorium comes into force pursuant to Schedule A1 of the Insolvency Act 1986; or

(h) any event similar to those listed in clauses H1.5 (a) to (g) occurs under the law of any other jurisdiction.

H1.6 References to the Insolvency Act 1986 in clause H1.5 (a) are references to that Act as applied under the Limited Liability Partnerships Act 2000 subordinate legislation.

H2 Default

H2.1 The Authority may terminate the Contract with immediate effect by notice if the Supplier commits a Default and:

(a) the Supplier has not remedied the Default to the satisfaction of the Authority within 20 Working Days or such other period as may be specified by the Authority, after issue of a notice specifying the Default and requesting it to be remedied;

(b) the Default is not, in the opinion of the Authority, capable of remedy; or

(c) the Default is a Material Breach.

H2.2 If, through any Default of the Supplier, data transmitted or processed in connection with the Contract is either lost or sufficiently degraded as to be unusable, the Supplier is liable for the cost of reconstitution of that data and shall reimburse the Authority in respect of any charge levied for its transmission and any other costs charged in connection with such Default.

H2.3 If the Authority fails to pay the Supplier undisputed sums of money when due, the Supplier shall give notice to the Authority of its failure to pay. If the Authority fails to pay such undisputed sums within 90 Working Days of the date of such notice, the Supplier may terminate the Contract with immediate effect, save that such right of termination shall not apply where the failure to pay is due to the Authority exercising its rights under clause C3.1 or to a Force Majeure Event.

H3 Termination on Notice

The Authority may terminate the Contract at any time by giving 90 days' notice to the Supplier.

H4 Other Grounds

H4.1 The Authority may terminate the Contract if:

(a) the Contract has been subject to a substantial modification which requires a new procurement procedure pursuant to regulation 72(9) of the Regulations;

(b) the Supplier was, at the time the Contract was awarded, in one of the situations specified in regulation 57(1) of the Regulations, including as a result of the application of regulation 57(2), and should therefore have been excluded from the procurement procedure which resulted in its award of the Contract;

(c) the Contract should not have been awarded to the Supplier in view of a serious infringement of the obligations under the Treaties and the Regulations that has been declared by the Court of Justice of the European Union in a procedure under Article 258 of the TFEU; or

(d) the Supplier has not, in performing the Services, complied with its legal obligations in respect of environmental, social or labour law.

H5 Consequences of Expiry or Termination

H5.1 If the Authority terminates the Contract under clause H2 and makes other arrangements for the supply of the Services the Authority may recover from the Supplier the cost reasonably incurred of making those other arrangements and any additional expenditure incurred by the Authority throughout the remainder of the Term.

H5.2 If the Contract is terminated under clause H2 the Authority shall make no further payments to the Supplier (for Services supplied by the Supplier prior to termination and in accordance with the Contract but where the payment has yet to be made by the Authority), until the Authority has established the final cost of making the other arrangements envisaged under this clause H5.

H5.3 If the Authority terminates the Contract under clauses H3 or H4 the Authority shall make no further payments to the Supplier except for Services supplied by the Supplier prior to termination and in accordance with the Contract but where the payment has yet to be made by the Authority.

H5.4 Save as otherwise expressly provided in the Contract:

(a) termination or expiry of the Contract shall be without prejudice to any rights, remedies or obligations accrued under the Contract prior to termination or expiration and nothing in the Contract prejudices the right of either Party to recover any amount outstanding at such termination or expiry; and

(b) termination of the Contract does not affect the continuing rights, remedies or obligations of the Authority or the Supplier under clauses C2 (Payment and VAT), C3 (Recovery of Sums Due), D2 (Data Protection and Privacy), D3 (Official Secrets Acts and Finance Act), D4 (Confidential Information), D5 (Freedom of Information), E1 (Intellectual Property Rights), F5 (Audit), G1 (Liability, Indemnity and Insurance), H5 (Consequences of Expiry or Termination), H7 (Recovery), H8 (Retendering and Handover), H9 (Exit Management), H10 (Knowledge Retention), I6 (Remedies Cumulative), I12 (Governing Law and Jurisdiction) and paragraph 9 of Schedule 8.

H6 Disruption

H6.1 The Supplier shall take reasonable care to ensure that in the performance of its obligations under the Contract it does not disrupt the operations of the Authority, its employees or any other contractor employed by the Authority.

H6.2 The Supplier shall immediately inform the Authority of any actual or potential industrial action, whether such action be by its own employees or others, which affects or might affect its ability at any time to perform its obligations under the Contract.

H6.3 If there is industrial action by Staff, the Supplier shall seek Approval for its proposals to continue to perform its obligations under the Contract.

H6.4 If the Supplier's proposals referred to in clause H6.3 are considered insufficient or unacceptable by the Authority acting reasonably, the Contract may be terminated with immediate effect by the Authority.

H6.5 If the Supplier is unable to deliver the Services owing to disruption of the Authority's normal business, the Supplier may request a reasonable allowance of time, and, in addition, the Authority will reimburse any additional expense reasonably incurred by the Supplier as a direct result of such disruption.

H7 Recovery

H7.1 On termination of the Contract for any reason, the Supplier shall at its cost:

(a) immediately return to the Authority all Confidential Information, Personal Data and IP Materials in its possession or in the possession or under the control of any permitted suppliers or Sub-Contractors, which was obtained or produced in the course of providing the Services;

(b) immediately deliver to the Authority all Property (including materials, documents, information and access keys) provided to the Supplier in good working order;

(c) Not used

(d) assist and co-operate with the Authority to ensure an orderly transition of the provision of the Services to the Replacement Supplier and/or the completion of any work in progress; and

(e) promptly provide all information concerning the provision of the Services which may reasonably be requested by the Authority for the purposes of adequately understanding the manner in which the Services have been provided and/or for the purpose of allowing the Authority and/or the Replacement Supplier to conduct due diligence.

H7.2 If the Supplier does not comply with clauses H7.1 (a) and (b), the Authority may recover possession thereof and the Supplier grants a licence to the Authority or its appointed agents to enter (for the purposes of such recovery) any premises of the Supplier or its suppliers or Sub-Contractors where any such items may be held.

H8 Retendering and Handover

H8.1 Within 21 days of being requested by the Authority, the Supplier shall provide, and thereafter keep updated, in a fully indexed and catalogued format, all the information necessary to enable the Authority to issue tender documents for the future provision of the Services.

H8.2 The Authority shall take all necessary precautions to ensure that the information referred to in clause H8.1 is given only to potential providers who have qualified to tender for the future provision of the Services.

H8.3 The Authority shall require that all potential providers treat the information in confidence; that they do not communicate it except to such persons within their organisation and to such extent as may be necessary for the purpose of preparing a response to an invitation to tender issued by the Authority; and that they shall not use it for any other purpose.

H8.4 The Supplier indemnifies the Authority against any claim made against the Authority at any time by any person in respect of any liability incurred by the Authority arising from any deficiency or inaccuracy in information which the Supplier is required to provide under clause H8.1.

H8.5 The Supplier shall allow access to the Premises in the presence of an authorised representative, to any person representing any potential provider whom the Authority has selected to tender for the future provision of the Services.

H8.6 If access is required to the Supplier's Premises for the purposes of clause H8.5, the Authority shall give the Supplier 7 days' notice of a proposed visit together with a list showing the names of all persons who will be visiting. Their attendance shall be subject to compliance with the Supplier's security procedures, subject to such compliance not being in conflict with the objectives of the visit.

H8.7 The Supplier shall co-operate fully with the Authority during any handover at the end of the Contract. This co-operation includes allowing full access to, and providing copies of, all documents, reports, summaries and any other information necessary in order to achieve an effective transition without disruption to routine operational requirements.

H8.8 Within 10 Working Days of being requested by the Authority, the Supplier shall transfer to the Authority, or any person designated by the Authority, free of charge, all computerised filing,

recording, documentation, planning and drawing held on software and utilised in the provision of the Services. The transfer shall be made in a fully indexed and catalogued disk format, to operate on a proprietary software package identical to that used by the Authority.

H9 Exit Management

H9.1 On termination of the Contract the Supplier shall render reasonable assistance to the Authority to the extent necessary to effect an orderly assumption by a Replacement Supplier in accordance with the procedure set out in clauses H9.2 to H9.5.

H9.2 If the Authority requires a continuation of all or any of the Services on expiry or termination of the Contract, either by performing them itself or by engaging a third party to perform them, the Supplier shall co-operate fully with the Authority and any such third party and shall take all reasonable steps to ensure the timely and effective transfer of the Services without disruption to routine operational requirements.

H9.3 The following commercial approach shall apply to the transfer of the Services if the Supplier:

(a) does not have to use resources in addition to those normally used to deliver the Services prior to termination or expiry, there shall be no change to the Price; or

(b) reasonably incurs additional costs, the Parties shall agree a Change to the Price based on the Supplier's rates either set out in Schedule 2 or forming the basis for the Price.

H9.4 When requested to do so by the Authority, the Supplier shall deliver to the Authority details of all licences for software used in the provision of the Services including the software licence agreements.

H9.5 Within one Month of receiving the software licence information described in clause H9.4, the Authority shall notify the Supplier of the licences it wishes to be transferred and the Supplier shall provide for the approval of the Authority a plan for licence transfer.

H10 Knowledge Retention

The Supplier shall co-operate fully with the Authority in order to enable an efficient and detailed knowledge transfer from the Supplier to the Authority on the completion or earlier termination of the Contract and in addition, to minimise any disruption to routine operational requirements. To facilitate this transfer, the Supplier shall provide the Authority free of charge with full access to its Staff, and in addition, copies of all documents, reports, summaries and any other information requested by the Authority. The Supplier shall comply with the Authority's request for information no later than 15 Working Days from the date that that request was made.

I GENERAL

I1 Dispute Resolution

I1.1 The Parties shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the Contract within 20 Working Days of either Party notifying the other of the dispute and such efforts shall involve the escalation of the dispute to the finance director of the Supplier and the commercial director of the Authority.

I1.2 Nothing in this dispute resolution procedure prevents the Parties seeking from any court of competent jurisdiction an interim order restraining the other Party from doing any act or compelling the other Party to do any act.

I1.3 If the dispute cannot be resolved by the Parties pursuant to clause I1.1 either Party may refer it to mediation pursuant to the procedure set out in clause I1.5.

I1.4 The obligations of the Parties under the Contract shall not cease, or be suspended or delayed by the reference of a dispute to mediation (or arbitration) and the Supplier and the Staff shall comply fully with the requirements of the Contract at all times.

I1.5 The procedure for mediation and consequential provisions relating to mediation are as follows:

(a) a neutral adviser or mediator (the "**Mediator**") shall be chosen by agreement of the Parties or, if they are unable to agree upon a Mediator within 10 Working Days after a request by one Party to the other or if the Mediator agreed upon is unable or unwilling to act, either Party shall within 10 Working Days from the date of the proposal to appoint a Mediator or within 10 Working Days of notice to either Party that he is unable or unwilling to act, apply to the Centre for Effective Dispute Resolution to appoint a Mediator;

(b) the Parties shall within 10 Working Days of the appointment of the Mediator meet with him in order to agree a programme for the exchange of all relevant information and the structure to be adopted for negotiations. If appropriate, the Parties may at any stage seek assistance from the Centre for Effective Dispute Resolution to provide guidance on a suitable procedure;

(c) unless otherwise agreed, all negotiations connected with the dispute and any settlement agreement relating to it shall be conducted in confidence and without prejudice to the rights of the Parties in any future proceedings;

(d) if the Parties reach agreement on the resolution of the dispute, the agreement shall be recorded in writing and shall be binding on the Parties once it is signed by their duly authorised representatives;

(e) failing agreement, either of the Parties may invite the Mediator to provide a non-binding but informative written opinion. Such an opinion shall be provided on a without prejudice basis and shall not be used in evidence in any proceedings relating to the Contract without the prior written consent of both Parties; and

(f) if the Parties fail to reach agreement within 60 Working Days of the Mediator being appointed, or such longer period as may be agreed by the Parties, then any dispute or difference between them may be referred to the Courts unless the dispute is referred to arbitration pursuant to the procedures set out in clause I1.6.

I1.6 Subject to clause I1.2, the Parties shall not institute court proceedings until the procedures set out in clauses I1.1 and I1.3 have been completed save that:

(a) the Authority may at any time before court proceedings are commenced, serve a notice on the Supplier requiring the dispute to be referred to and resolved by arbitration in accordance with clause I1.7;

(b) if the Supplier intends to commence court proceedings, it shall serve notice on the Authority of its intentions and the Authority has 21 days following receipt of such notice to serve a reply on the Supplier requiring the dispute to be referred to and resolved by arbitration in accordance with clause I1.7; and

(c) the Supplier may request by notice to the Authority that any dispute be referred and resolved by arbitration in accordance with clause I1.7, to which the Authority may consent as it sees fit.

I1.7 If any arbitration proceedings are commenced pursuant to clause I1.6:

(a) the arbitration is governed by the Arbitration Act 1996 and the Authority shall give a notice of arbitration to the Supplier (the "**Arbitration Notice**") stating:

(i) that the dispute is referred to arbitration; and

(ii) providing details of the issues to be resolved;

(b) the London Court of International Arbitration ("**LCIA**") procedural rules in force at the date that the dispute was referred to arbitration in accordance with I1.7 (b) shall be applied and are deemed to be incorporated by reference to the Contract and the decision of the arbitrator is binding on the Parties in the absence of any material failure to comply with such rules;

(c) the tribunal shall consist of a sole arbitrator to be agreed by the Parties;

(d) if the Parties fail to agree the appointment of the arbitrator within 10 days of the Arbitration Notice being issued by the Authority under clause I1.7 (a) or if the person appointed is unable or unwilling to act, the arbitrator shall be appointed by the LCIA;

(e) the arbitration proceedings shall take place in London and in the English language; and

(f) the arbitration proceedings shall be governed by, and interpreted in accordance with, English Law.

I2 Force Majeure

I2.1 Subject to this clause I2, a Party may claim relief under this clause I2 from liability for failure to meet its obligations under the Contract for as long as and only to the extent that the performance of those obligations is directly affected by a Force Majeure Event. Any failure or delay by the Supplier in performing its obligations under the Contract which results from a failure or delay by an agent, Sub-Contractor or supplier is regarded as due to a Force Majeure Event only if that agent, Sub-Contractor or supplier is itself impeded by a Force Majeure Event from complying with an obligation to the Supplier.

I2.2 The Affected Party shall as soon as reasonably practicable issue a Force Majeure Notice, which shall include details of the Force Majeure Event, its effect on the obligations of the Affected Party and any action the Affected Party proposes to take to mitigate its effect.

I2.3 If the Supplier is the Affected Party, it is not entitled to claim relief under this clause I2 to the extent that consequences of the relevant Force Majeure Event:

(a) are capable of being mitigated by any of the Services, but the Supplier has failed to do so; and/or

(b) should have been foreseen and prevented or avoided by a prudent provider of services similar to the Services, operating to the standards required by the Contract.

I2.4 Subject to clause I2.5, as soon as practicable after the Affected Party issues the Force Majeure Notice, and at regular intervals thereafter, the Parties shall consult in good faith and use reasonable endeavours to agree any steps to be taken and an appropriate timetable in which those steps should be taken, to enable continued provision of the Services affected by the Force Majeure Event.

I2.5 The Parties shall at all times following the occurrence of a Force Majeure Event and during its subsistence use their respective reasonable endeavours to prevent and mitigate the effects of the Force Majeure Event. Where the Supplier is the Affected Party, it shall take all steps in accordance with Good Industry Practice to overcome or minimise the consequences of the Force Majeure Event.

I2.6 If, as a result of a Force Majeure Event:

(a) an Affected Party fails to perform its obligations in accordance with the Contract, then during the continuance of the Force Majeure Event:

i) the other Party is not entitled to exercise its rights to terminate the Contract in whole or in part as a result of such failure pursuant to clause H2.1 or H2.3; and

ii) neither Party is liable for any Default arising as a result of such failure;

(b) the Supplier fails to perform its obligations in accordance with the Contract it is entitled to receive payment of the Price (or a proportional payment of it) only to the extent that the Services (or part of the Services) continue to be performed in accordance with the Contract during the occurrence of the Force Majeure Event.

I2.7 The Affected Party shall notify the other Party as soon as practicable after the Force Majeure Event ceases or no longer causes the Affected Party to be unable to comply with its obligations under the Contract.

I2.8 Relief from liability for the Affected Party under this clause I2 ends as soon as the Force Majeure Event no longer causes the Affected Party to be unable to comply with its obligations under the Contract and is not dependent on the serving of a notice under clause I2.7.

I3 Notices and Communications

I3.1 Subject to clause I3.3, where the Contract states that a notice or communication between the Parties must be "written" or "in writing" it is not valid unless it is made by letter (sent by hand, first class post, recorded delivery or special delivery) or by email or by communication via Bravo.

I3.2 If it is not returned as undelivered a notice served in:

(a) a letter is deemed to have been received 2 Working Days after the day it was sent; and

(b) an email is deemed to have been received 4 hours after the time it was sent provided it was sent on a Working Day

or when the other Party acknowledges receipt, whichever is the earlier.

I3.3 Notices pursuant to clauses I1, I2 or I7 or to terminate the Contract or any part of the Services are valid only if served in a letter by hand, recorded delivery or special delivery.

I3.4 Notices shall be sent to the addresses set out below or at such other address as the relevant Party may give notice to the other Party for the purpose of service of notices under the Contract:

(a) For the Authority:

Contact Name: Redacted Under FOIA Section 43

(b) For the Supplier:

Contact Name: Redacted Under FOIA Section 43

I4 Conflicts of Interest

I4.1 The Supplier shall take appropriate steps to ensure that neither the Supplier nor any Staff is placed in a position where, in the reasonable opinion of the Authority, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Supplier and the duties owed to the Authority under the Contract. The Supplier will notify the Authority immediately giving full particulars of any such conflict of interest which may arise.

I4.2 The Authority may terminate the Contract immediately by notice and/or take or require the Supplier to take such other steps it deems necessary if, in the Authority's reasonable opinion, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Supplier and the duties owed to the Authority under the Contract. The actions of the Authority pursuant to this clause I4 shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereafter accrue to the Authority.

I5 Rights of Third Parties

I5.1 Clauses B10.5 and E1.3 confer benefits on persons named in them (together "**Third Party Provisions**" and each person a "**Third Party Beneficiary**") other than the Parties and are intended to be enforceable by Third Party Beneficiaries by virtue of the Contracts (Rights of Third Parties) Act 1999 ("**CRTPA**").

I5.2 Subject to clause I5.1, a person who is not a Party has no right under the CRTPA to enforce the Contract but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to the CRTPA and does not apply to the Crown.

I5.3 No Third-Party Beneficiary may enforce or take steps to enforce any Third-Party Provision without Approval.

I5.4 Any amendments to the Contract may be made by the Parties without the consent of any Third-Party Beneficiary.

I6 Remedies Cumulative

Except as expressly provided in the Contract all remedies available to either Party for breach of the Contract are cumulative and may be exercised concurrently or separately, and the exercise of any one remedy are not an election of such remedy to the exclusion of other remedies.

I7 Waiver

I7.1 The failure of either Party to insist upon strict performance of any provision of the Contract, or the failure of either Party to exercise, or any delay in exercising, any right or remedy do not constitute a waiver of that right or remedy and do not cause a diminution of the obligations established by the Contract.

I7.2 No waiver is effective unless it is expressly stated to be a waiver and communicated to the other Party in writing in accordance with clause I3 (Notices and Communications).

I7.3 A waiver of any right or remedy arising from a breach of the Contract does not constitute a waiver of any right or remedy arising from any other or subsequent breach of the Contract.

I8 Severability

If any part of the Contract which is not of a fundamental nature is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such part shall be severed and the remainder of the Contract shall continue in full effect as if the Contract had been executed with the invalid, illegal or unenforceable part eliminated.

I9 Entire Agreement

The Contract constitutes the entire agreement between the Parties in respect of the matters dealt with therein. The Contract supersedes all prior negotiations between the Parties and all representations and undertakings made by one Party to the other, whether written or oral, except that this clause shall not exclude liability in respect of any fraudulent misrepresentation.

I10 Change in Law

I10.1 The Supplier is neither relieved of its obligations to supply the Services in accordance with the terms and conditions of the Contract nor entitled to an increase in the Price as the result of:

(a) a General Change in Law; or

(b) a Specific Change in Law where the effect of that Specific Change in Law on the Services is reasonably foreseeable at the Commencement Date.

I10.2 If a Specific Change in Law occurs or will occur during the Term (other than as referred to in clause I10.1(b)), the Supplier shall:

(a) notify the Authority as soon as reasonably practicable of the likely effects of that change, including whether any:

(i) Change is required to the Services, the Price or the Contract; and
(ii) relief from compliance with the Supplier's obligations is required; and

(b) provide the Authority with evidence:

(i) that the Supplier has minimised any increase in costs or maximised any reduction in costs, including in respect of the costs of its Sub-Contractors; and

(ii) as to how the Specific Change in Law has affected the cost of providing the Services.

I10.3 Any variation in the Price or relief from the Supplier's obligations resulting from a Specific Change in Law (other than as referred to in clause I10.1(b)) shall be implemented in accordance with clause F4.

I11 Counterparts

The Contract may be executed in counterparts, each of which when executed and delivered constitute an original but all counterparts together constitute one and the same instrument.

I12 Governing Law and Jurisdiction

Subject to clause I1 (Dispute Resolution) the Contract, including any matters arising out of or in connection with it, are governed by and interpreted in accordance with English Law and are subject to the jurisdiction of the Courts of England and Wales. The submission to such jurisdiction does not limit the right of the Authority to take proceedings against the Supplier in any other court of competent jurisdiction, and the taking of proceedings in any other court of competent jurisdiction does not preclude the taking of proceedings in any other jurisdiction whether concurrently or not.

A. The Service - Service Overview

1. The Supplier will provide support to offenders under probation supervision that have been referred to the Supplier by the Authority.

2. The Supplier will provide each resident referred to the Supplier by the Authority with a minimum of 6 hours of purposeful activity per week, interventions designed to address both complex offence related need and risk.

3. The Supplier will accept referrals and provide bed spaces at the locations set out in appendix 3. The Authority acknowledges that this is not exclusive access and in the case of Care homes referrals would only be accepted once the appropriate funding has been secured.

4. The Supplier will manage a national referral procedure in agreement with the Authority.

5. The Supplier will provide an initial assessment of the resident's accommodation and support needs on admission and the assessment will be reviewed by the Supplier on a quarterly basis whilst the offender is resident with the Supplier and under statutory supervision by the National Probation Service.

6. The Supplier will provide the Services in accordance with all relevant legislation, standards, Probation Instructions and guidance including the Approved Premises Manual. Probation Instructions can be viewed and downloaded at https://www.justice.gov.uk/offenders/probation-instructions and A link to the Approved Premises Manual is attached in Appendix 1.

7. The Supplier will contribute to the Probation Service Probation Practitioner's sentence plan in working to reduce offending behaviour and manage risk.

8. The Supplier will work on practical difficulties experienced by the offender and help them to develop the life and social skills necessary for independent living.

9. The Supplier will help the offender link into or maintain sources of continuing support and assistance in the community.

10. The Supplier will contribute to the assessment of the offender's ability to live independently. Where living independently is part of the offender's sentence plan, the Supplier will assist the offender to achieve this objective.

11. The Supplier shall notify the Probation Practitioner of any known breaches of licencing conditions or community orders by residents as soon as is reasonably possible.

B. Operational

1. The Supplier shall, in respect of all provision under this contract:

1.1. Maintain up to date records of House Rules, ensure all offenders agree to and sign the House Rules on admission and regularly monitor residents to ensure that the house Rules are enforced. Should there be any conflict between and any licence conditions that residents are subject to then the licence conditions shall prevail;

The NPS Offender Manager is responsible for making decisions regarding the breach and recall of offenders. The Supplier is required to assist the Probation Service in the process of making decisions regarding breach/recall by providing information, objective feedback and dynamic assessment of the risks and challenges presented. The Supplier must have robust and flexible arrangements in place for effectively managing residents behaviour, for enforcing expectations, for engaging with the multiple and complex problems experienced by residents and for escalation to NPS where appropriate. Suppliers must report on the levels of breach/recall via the agreed process as set out in the AP manual.

1.2. Co-operate with the NPS out-of-hours on-call arrangements where recall or breach needs are required outside of office hours. The NPS will provide the Supplier with details of the out of hours duty manager rota and contact details. There will an NPS AP manager on duty out of hours in each area who will be available for discussion and who is delegated authority on behalf of the Secretary of State for Justice to make decisions with regard to recall. Recall decisions for offenders who are subject to Multi Agency Public Protection Arrangements ("MAPPA") Level 3, Life Licence or an Indeterminate Sentence for Public Protection (IPP) must be made by an NPS Head of Operational Service (formerly Assistant Chief Officer) and the NPS AP manager on call will facilitate this.

1.3. Provide:

a) to all MAPPA eligible residents (regardless of level) or those allocated to a 24-hour staffed placement, a minimum of 6 hours purposeful activities per week

for the first 12 weeks of residence, unless agreed otherwise by the Offender Manager and the Authority Contract Manager.

b) to all other residents, a minimum of 1 hour of purposeful activities per week to for the first 12 weeks of residence.

After the first 12 weeks of residence, these requirements will be reviewed and agreed in collaboration with the Authority on a needs-led basis. The activities must tackle criminogenic need and promote rehabilitation; Suppliers will be expected to evidence delivery of purposeful activity as per agreed reporting mechanisms. This will include evidence of weekly activity/group-work timetables. All purposeful activities must be able to demonstrate that they are linked to one or more of the 9 offender pathways. Full time employment or full time voluntary work of over 37 hours will be counted as purposeful activity.

1.4. Maintain a regime consisting of purposeful, constructive activities designed to manage risk, tackle criminogenic need and promote rehabilitation;

1.5. Maintain up to date records of residents entering and leaving the premises that can be used for monitoring MAPPA residents as part of their compliance (only refers to settings with 24/7 staffing).

1.6. Ensure that robust systems are in place on each site for monitoring MAPPA residents entering and leaving the premises (only refers to settings with 24/7 staffing);

1.7. NOT USED

1.8. Provide suitable facilities with a structured regime and staffing that provide a service to meet the needs of all relevant offender groups and cater for their diverse needs;

1.9. Provide facilities, a regime and a staff team that are accessible to all relevant offender groups and cater for their diverse needs;

1.10. NOT USED

1.11. Recruit and employ adequate and appropriate staff deployment, and appropriate security measures, linked to the resident profile of each unit.

1.12. Arrange adequate and appropriate staff deployment, and appropriate security measures, linked to the resident profile of each unit.

1.13. Organise attendance for the supplier's hostel managers to attend any relevant local NPS Divisional management meetings to which they are invited;

1.14. Make the necessary arrangements for managers and staff to have access to and attend training provided in the local NPS Division;

1.15. Ensure that managers and staff can access training opportunities provided in the local NPS Division;

1.16. Develop, monitor and maintain a strategy for managing the risks of suicide and self-harm, in line with the guidance provided in the Approved Premises manual (please see attached manual in Appendix 1 to this Contract)

1.17. Develop, monitor and maintain a Health and Safety Policy that complies with all relevant health and safety legislation. Ensure the policy is made available to and agreed with the relevant NPS Division.

1.18. Establish written contingency arrangements, agreed with the relevant NPS Division, in the event of a major incident requiring full or partial closure of the Supplier's premises; establish management systems to co-ordinate the arrangements and provide a named person for contact; and establish national contingency arrangements for a major incident affecting all of the Supplier's accommodation or the Supplier itself as an entity.

2. Complaints

The Supplier shall, in respect of all provision under this contract:

2.1. Maintain an up to date complaints policy and procedure for the handling of complaints, written and verbal, from residents, neighbours or other third parties and regularly review for each hostel;

2.2. In the event of a complaint being made by the Customer or one of its employees about the quality or level of service provision, the Supplier will investigate the complaint and respond in writing with the outcome of that investigation. If the complaint cannot be resolved within that timeframe, the Supplier must send an interim response giving reasons for the delay and the likely timeframe for resolution.

2.3. Unresolved complaints will be reviewed at the Customer's quarterly Contract meeting.

2.4. An escalation process should be established available where necessary and this should be 3 stages:

2.4.1. Level One Account Manager
2.4.2. Level Two Director
2.4.3. Level Three Board of Directors

3. Audit and inspection

The Supplier shall, in respect of all provision under this contract:

3.1. Develop a range of performance standards, to carry out service delivery audits on each site and to produce improvement plans for each property based on the results in agreement with the Authority Contract Manager; and

3.2. Participate in, co-operate with and provide feedback with audits and inspections, internal or external, bi – annual and as required, including investigations by the Prisons & Probation Ombudsman.

4. Accommodation

4.1 Service level

In addition to the responsibilities set out above, in respect of accommodation the supplier shall:

4.1.1. Provide places for MAPPA Level 2 and Level 3 offenders, prioritising those who are moving on from Approved Premises;

4.1.2. Provide additional places for a range of other offenders subject to probation supervision; and

4.1.3. Maintain an admissions policy compliant with PI 32/2014 (Please note Probation Instructions can be access on the Justice website:

https://www.justice.gov.uk/offenders/probation-instructions) and that reflects the Strategic Purpose of the Agreement;

4.2 Guidance

In addition to the responsibilities set out above, in respect of accommodation the supplier shall:

4.2.1 Maintain guidance for its staff setting out the respective responsibilities of the Authority's and the supplier's staff in respect of referrals, admissions and offender management;

4.3 Performance Reporting

In addition to the responsibilities set out above, in respect of accommodation the supplier shall:

4.3.1 provide monthly performance reporting as set out in Appendix 2 to this Schedule 1, no later than ten working days following the end of the calendar month of reporting;

4.3.2 submit an Annual Report by 31 March 2022 for contract year 1 and 31 March 2023 for contract year 2, and 31 March 2024 for contract year 3 that provides a strategic overview of the individual monthly performance reports for the year; and

4.3.2 Attend meetings convened by the Authority, as reasonably required. This will consist of quarterly formal contract reviews and biannual site visits.

Appendix 1A – House Rules

Redacted Under FOIA Section 43

Appendix 1 – Approved Premises Manual

pi_32_2014_annex_
a_approve_premises

Available at: https://www.justice.gov.uk/downloads/offenders/probation-instructions/pi-32-2014-annex-a-approved-premises-manual.doc

Appendix 2 – Performance reporting

In accordance with Schedule 1 Section 4.3.1 the monthly performance reports must encompass:

1) Referrals to Redacted Under FOIA Section 43 from the Probation Service by month [by Probation Service region/Division]
2) Referrals from, i.e. the location they move from into Redacted Under FOIA Section 43, e.g. prison, Approved Premises, community, Mental Health Ward etc
3) Entries into Redacted Under FOIA Section 43from the Probation Service by month [by Probation Service region/division]
4) Entries into Redacted Under FOIA Section 43 by main offence
5) Entries into Redacted Under FOIA Section 43 by complexity [i.e. by additional care needs over and above a bed or the "basic" level]
6) Departures by month
7) Departures by length of stay
8) Departures where to, e.g. Approved Premises, Community, specialist provision, residential home etc
9) Case studies to be provided at quarterly meetings.

10) Breakdown of referral type including Protected characteristics &
11) Breakdown of referral by MAPPA level

Appendix 3 – List of in-scope projects and accommodation

Redacted Under FOIA Section 43

Part 1 Charges & Milestone Payments

1.1. The total charges payable by the Authority to the Supplier under this contract are £Redacted Under FOIA Section 43 annum for year one of the contract. Years 2 and 3 will be confirmed following Consumer Price indexation.

Indexation Review Date" means 1 April of each year from Contract Year 2 onwards

1.2. Payments will be made monthly in arrears as per the following schedule:

Redacted Under FOIA Section 43

Part 2 Indexation

2.1 On each Indexation Review Date, the pricing elements set out in this Schedule 2 (**PRICES and INVOICING**) may be subject to indexation in line with Consumer Price Index from the ONS official published rates.

2.2 The Supplier shall calculate the indexation, using the indicies published three months preceding the Indexation Review Date, against the cost template and share with the Authority.

2.3 The Supplier shall confirm to the Authority that any increases to the Price would be proportionate to the uplift in actual contract running costs and provide additional evidence if requested to by the Authority.

2.4 Subject to clause 3.1, upon receipt of the above update as per 3.2, the Authority will assure the calculations and the change to the Price will take effect from the Indexation Review Date.

Part 3 Invoicing

3.1 The Supplier shall register on Basware eMarketplace set out in Annex 1 to this schedule 2.

3.2 The Supplier shall submit to the Authority an electronic invoice via the Basware supplier portal (as per Annex 1) for the agreed amount within 10 working days of the invoice due date as shown at part 1 section 1.2 above.

3.3 In accordance with clause C1.15, payment will be made by the Authority via Electronic Funds Transfer (BACS) within 30 days of receipt of a Valid Invoice, submitted electronically.

Part 4 Open book accounting

4.1 The Authority and the Supplier agree to adopt an open-book accounting approach to the financial management of this Contract.

4.2 The Authority may request financial information from the Supplier to evidence the costs incurred by the Supplier in carrying out the services under this contract including but not limited to the following;

a) Audited financial accounts

b) Bank statements

c) Financing arrangements

d) Payroll information

e) Supplementary information (invoices, receipts, tax returns)

f) Financial management information (cash flow forecasts, budgets)

g) Any other information reasonably requested by the Authority to demonstrate the financial viability and sustainability of the Supplier and its performance of the services under this contract.

4.3 Guidance from the National Audit Office in regard to the use of open-book accounting can be accessed via the following link.

https://www.nao.org.uk/wp-content/uploads/2015/07/Open-book-accounting.pdf

Annex 1 Basware eMarketplace guidance

SCHEDULE 3 - CHANGE CONTROL

Change Request Form
(For completion by the Party requesting the Change)

Contract Title:	**Party requesting Change:**
Name of Supplier:	
Change Request Number:	**Proposed Change implementation date:**
Full description of requested Change (including proposed changes to wording of the Contract where possible):	

Reasons for requested Change:
Effect of requested Change
Assumptions, dependencies, risks and mitigation (if any):
Change Request Form prepared by (name):
Signature:
Date of Change Request:

Contract Change Notice ("CCN")

(For completion by the Authority once the Change has been agreed in principle by both Parties. Changes do not become effective until this form has been signed by both Parties.)

Contract Title:	**Change requested by:**
Name of Supplier:	
Change Number:	
Date on which Change takes effect:	
Contract between: The [Secretary of State for Justice]/[The Lord Chancellor] [delete as applicable] and [insert name of Supplier]	

It is agreed that the Contract is amended, in accordance with Regulation 72 of the Public Contracts Regulations 2015, as follows: [Insert details of the variation (including any change to the Price and deliverables/obligations) based on the information provided in the Change Request Form and any subsequent discussions/negotiations, cross referencing the wording of the original Contract, as previously changed (if applicable), where possible] **Where significant changes have been made to the Contract, information previously published on Contracts Finder will be updated.**
Words and expressions in this CCN shall have the meanings given to them in the Contract. The Contract, including any previous CCNs, shall remain effective and unaltered except as amended by this CCN

Signed for and on behalf of [the Secretary of State for Justice]/[the Lord Chancellor]		**Signed for and on behalf of** [Insert name of Supplier]	
Signature		**Signature**	
Name		**Name**	
Title		**Title**	
Date		**Date**	

SCHEDULE 4 - COMMERCIALLY SENSITIVE INFORMATION

1 Without prejudice to the Authority's general obligation of confidentiality, the Parties acknowledge that the Authority may have to disclose Information in or relating to the Contract following a Request for Information pursuant to clause D5 (Freedom of Information).

2 In this Schedule 4 the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be contrary to the public interest.

3 Where possible the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule 4 applies.

4 Without prejudice to the Authority's obligation to disclose Information in accordance with the FOIA and the EIR, the Authority will, acting reasonably but in its sole discretion, seek to apply the commercial interests exemption set out in s.43 of the FOIA to the Information listed below.

SUPPLIER'S COMMERCIALLY SENSITIVE INFORMATION	DATE	DURATION OF CONFIDENTIALITY
Contract Price, financial reports, accounts etc		For the Term of the Contract and six years there after
All technical solution information as to the Supplier's delivery of services (trade secrets essentially)		For the Term of the Contract

SCHEDULE 5 - SUPPLIER AND THIRD PARTY SOFTWARE

Supplier Software comprises the following:

Software	Supplier (if Affiliate of the Supplier)	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?
N/A							

Third Party Software comprises the following:

Redacted Under FOIA Section 43

SCHEDULE 6 – INFORMATION ASSURANCE & SECURITY

1. GENERAL

1.1 This Schedule 6 sets out the obligations of the Parties in relation to information assurance and security, including those which the Supplier must comply with in delivering the Services under the Contract.

1.2 The Parties acknowledge that the purpose of the ISMS and Security Plan is to ensure a robust organisational approach to information assurance and security under which the specific requirements of the Contract will be met.

1.3 The Parties shall each appoint and/or identify a board level individual or equivalent who has overall responsibility for information assurance and security, including personnel security and information risk. The individual appointed by the Supplier, who is the Chief Security Officer, Chief Information Officer, Chief Technical Officer or equivalent and is responsible for compliance with the ISMS, is identified as Key Personnel) and the provisions of clause B4 apply in relation to that person.

1.4 The Supplier shall act in accordance with Good Industry Practice in the day to day operation of any system which is used for the storage of Information Assets and/or the storage, processing or management of Authority Data and/or that could directly or indirectly affect Information Assets and/or Authority Data.

1.5 The Supplier shall ensure that an information security policy is in place in respect of the operation of its organisation and systems, which shall reflect relevant control objectives for the Supplier System, including those specified in the ISO27002 control set or equivalent, unless otherwise agreed by the Authority. The Supplier shall, upon request, provide a copy of this policy to the Authority as soon as reasonably practicable. The Supplier shall maintain and keep such policy updated and provide clear evidence of this as part of its Security Plan.

1.6 The Supplier acknowledges that a compromise of Information Assets and/or Authority Data represents an unacceptable risk to the Authority requiring immediate communication and co-operation between the Parties. The Supplier shall provide clear evidence of regular communication with the Authority in relation to information risk as part of its Security Plan.

2. INFORMATION SECURITY MANAGEMENT SYSTEM

2.1 The Supplier shall, within 30 Working Days of the Commencement Date, submit to the Authority a proposed ISMS which:

2.1.1 has been tested; and

2.1.2 complies with the requirements of paragraphs 2.2 and 2.3.

2.2 The Supplier shall at all times ensure that the level of security, include cyber security, provided by the ISMS is sufficient to protect the confidentiality, integrity and availability of Information Assets and Authority Data used in the provision of the Services and to provide robust risk management.

2.3 The Supplier shall implement, operate and maintain an ISMS which shall:

2.3.1 protect all aspects of and processes of Information Assets and Authority Data, including where these are held on the ICT Environment (to the extent that this is under the control of the Supplier);

2.3.2 be aligned to and compliant with the relevant standards in ISO/IEC 27001: 2013 or equivalent and the Certification Requirements in accordance with paragraph 5 unless otherwise Approved;

2.3.3 provide a level of security which ensures that the ISMS and the Supplier System:

2.3.3.1 meet the requirements in the Contract;

2.3.3.2 are in accordance with applicable Law;

2.3.3.3 demonstrate Good Industry Practice, including the Government's 10 Steps to Cyber Security, currently available at:

https://www.ncsc.gov.uk/guidance/10-steps-cyber-security;

2.3.3.4 comply with the Security Policy Framework and any other relevant Government security standards;

2.3.3.5 comply with the Baseline Security Requirements;

2.3.3.6 comply with the Authority's policies, including, where applicable, the Authority's Information Assurance Policy in PSI 24/2014;

2.3.4 address any issues of incompatibility with the Supplier's organisational security policies;

2.3.5 address any specific security threats of immediate relevance to Information Assets and/or Authority Data;

2.3.6 document:

2.3.6.1 the security incident management processes, including reporting, recording and management of information risk incidents, including those relating to the ICT Environment (to the extent that this is within the control of the Supplier) and the loss of protected Personal Data, and the procedures for reducing and raising awareness of information risk;

2.3.6.2 incident response plans, including the role of nominated security incident response companies; and

2.3.6.3 the vulnerability management policy, including processes for identification of system vulnerabilities and assessment of the potential effect on the Services of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing and application of security patches and the reporting and audit mechanism detailing the efficacy of the patching policy;

2.3.7 include procedures for the secure destruction of Information Assets and Authority Data and any hardware or devices on which such information or data is stored; and

2.3.8 be certified by (or by a person with the direct delegated authority of) the Supplier's representative appointed and/or identified in accordance with paragraph 1.3.

2.4 If the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies notified to the Supplier from time to time, the Supplier shall immediately notify the Authority of such inconsistency and the Authority shall, as soon as practicable, notify the Supplier of the provision that takes precedence.

2.5 The Supplier shall, upon request from the Authority or any accreditor appointed by the Authority, provide sufficient design documentation detailing the security architecture of its ISMS to support the Authority's and/or accreditor's assurance that it is appropriate, secure and complies with the Authority's requirements.

2.6 The Authority shall review the proposed ISMS submitted pursuant to paragraph 2.1and shall, within 10 Business Days of its receipt notify the Supplier as to whether it has been approved.

2.7 If the ISMS is Approved, it shall be adopted by the Supplier immediately and thereafter operated and maintained throughout the Term in accordance with this Schedule 6.

2.8 If the ISMS is not Approved, the Supplier shall amend it within 10 Business Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Authority shall, within a further 10 Working Days notify the Supplier whether the amended ISMS has been approved. The Parties shall use reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 30 Working Days from the date of its first submission to the Authority. If the Authority does not approve the ISMS following its resubmission, the matter shall be resolved in accordance with clause I1 (Dispute Resolution).

2.9 Approval of the ISMS or any change to it shall not relieve the Supplier of its obligations under this Schedule 6.

2.10 The Supplier shall provide to the Authority, upon request, any or all ISMS documents.

3. SECURITY PLAN

3.1 The Supplier shall, within 30 Working Days of the Commencement Date, submit to the Authority for approval a Security Plan which complies with paragraph 3.2.

3.2 The Supplier shall effectively implement the Security Plan which shall:

3.2.1 comply with the Baseline Security Requirements;

3.2.2 identify the organisational roles for those responsible for ensuring the Supplier's compliance with this Schedule 6;

3.2.3 detail the process for managing any security risks from those with access to Information Assets and/or Authority Data, including where these are held in the ICT Environment;

3.2.4 set out the security measures and procedures to be implemented by the Supplier, which are sufficient to ensure compliance with the provisions of this Schedule 6;

3.2.5 set out plans for transition from the information security arrangements in place at the Commencement Date to those incorporated in the ISMS;

3.2.6 set out the scope of the Authority System that is under the control of the Supplier;

3.2.7 be structured in accordance with ISO/IEC 27001: 2013 or equivalent unless otherwise Approved;

3.2.8 be written in plain language which is readily comprehensible to all Staff and to Authority personnel engaged in the Services and reference only those documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule 6; and

3.2.9 comply with the Security Policy Framework and any other relevant Government security standards.

3.3 The Authority shall review the Security Plan submitted pursuant to paragraph 3.1 and notify the Supplier, within 10 Business Days of receipt, whether it has been approved.

3.4 If the Security Plan is Approved, it shall be adopted by the Supplier immediately and thereafter operated and maintained throughout the Term in accordance with this Schedule 6.

3.5 If the Security Plan is not Approved, the Supplier shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Authority shall notify the Supplier within a further 10 Business Days whether it has been approved.

3.6 The Parties shall use reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 30 Working Days from the date of its first submission to the Authority. If the Authority does not approve the Security Plan following its resubmission, the matter shall be resolved in accordance with clause I1 (Dispute Resolution).

3.7 Approval by the Authority of the Security Plan pursuant to paragraph 3.3 or of any change to the Security Plan shall not relieve the Supplier of its obligations under this Schedule 6.

4. REVISION OF THE ISMS AND SECURITY PLAN

4.1 The ISMS and Security Plan shall be reviewed in full and tested by the Supplier at least annually throughout the Term (or more often where there is a significant change to the Supplier System or associated processes or where an actual or potential Breach of Security or weakness is identified) to consider and take account of:

4.1.1 any issues in implementing the Security Policy Framework and/or managing information risk;

4.1.2 emerging changes in Good Industry Practice;

4.1.3 any proposed or actual change to the ICT Environment and/or associated processes;

4.1.4 any new perceived, potential or actual security risks or vulnerabilities;

4.1.5 any ISO27001: 2013 audit report or equivalent produced in connection with the Certification Requirements which indicates concerns; and

4.1.6 any reasonable change in security requirements requested by the Authority.

4.2 The Supplier shall give the Authority the results of such reviews as soon as reasonably practicable after their completion, which shall include without limitation:

4.2.1 suggested improvements to the effectiveness of the ISMS, including controls;

4.2.2 updates to risk assessments; and

4.2.3 proposed modifications to respond to events that may affect the ISMS, including the security incident management processes, incident response plans and general procedures and controls that affect information security.

4.3 Following the review in accordance with paragraphs 4.1 and 4.2 or at the Authority's request, the Supplier shall give the Authority at no additional cost a draft updated ISMS and/or Security Plan which includes any changes the Supplier proposes to make to the ISMS or Security Plan. The updated ISMS and/or Security Plan shall, unless otherwise agreed by the Authority, be subject to clause F4 (Change) and shall not be implemented until Approved.

4.4 If the Authority requires any updated ISMS and/or Security Plan to be implemented within shorter timescales than those set out in clause F4, the Parties shall thereafter follow clause F4 for the purposes of formalising and documenting the relevant change for the purposes of the Contract.

5. CERTIFICATION REQUIREMENTS

5.1 The Supplier shall ensure that any systems, including the ICT Environment, on which Information Assets and Authority Data are stored and/or processed are certified as compliant with:

5.1.1 ISO/IEC 27001:2013 or equivalent by a UKAS approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013 or equivalent unless otherwise Approved; and

5.1.2 the Government's Cyber Essentials Scheme at the BASIC level unless otherwise agreed with the Authority

and shall provide the Authority with evidence:

5.1.3 of certification before the Supplier accessed the ICT Environment and receives, stores, processes or manages any Authority Data; and

5.1.4 that such certification remains valid and is kept up to date while the Supplier(as applicable) continues to access the ICT Environment and receives, stores, processes or manages any Authority Data during the Term.

5.2 The Supplier shall ensure that it:

5.2.1 carries out any secure destruction of Information Assets and/or Authority Data at Supplier sites which are included within the scope of an existing certificate of compliance with ISO/IEC 27001:2013 or equivalent unless otherwise Approved; and

5.2.2 is certified as compliant with the CESG Assured Service (CAS) Service Requirement Sanitisation Standard or equivalent unless otherwise Approved

and the Supplier shall provide the Authority with evidence of its compliance with the requirements set out in this paragraph 5.2 before the Supplier may carry out the secure destruction of any Information Assets and/or Authority Data.

5.3 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier ceases to be compliant with the certification requirements in paragraph 5.1 and, on request from the Authority, shall:

5.3.1 immediately cease access to and use of Information Assets and/or Authority Data; and

5.3.2 promptly return, destroy and/or erase any Authority Data in accordance with the Baseline Security Requirements and failure to comply with this obligation is a material Default.

6. SECURITY TESTING

6.1 The Supplier shall, at its own cost, carry out relevant Security Tests from the Commencement Date and throughout the Term, which shall include:

6.1.1 a monthly vulnerability scan and assessment of the Supplier System and any other system under the control of the Supplier on which Information Assets and/or Authority Data are held;

6.1.2 an annual IT Health Check by an independent CHECK qualified company of the Supplier System and any other system under the control of the Supplier on which Information Assets and/or Authority Data are held and any additional IT Health Checks required by the Authority and/or any accreditor;

6.1.3 an assessment as soon as reasonably practicable following receipt by the Supplier of a critical vulnerability alert from a provider of any software or other component of the Supplier System and/or any other system under the control of the Supplier on which Information Assets and/or Authority Data are held; an

6.1.4 such other tests as are required:

6.1.4.1 by any Vulnerability Correction Plans;

6.1.4.2 by ISO/IEC 27001:2013 certification requirements or equivalent Approved;

6.1.4.3 after any significant architectural changes to the ICT Environment;

6.1.4.4 after a change to the ISMS (including security incident management processes and incident response plans) or the Security Plan; and

6.1.4.5 following a Breach of Security.

6.2 In relation to each IT Health Check, the Supplier shall:

6.2.1 agree with the Authority the aim and scope of the IT Health Check;

6.2.2 promptly, following receipt of each IT Health Check report, give the Authority a copy of the IT Health Check report;

6.2.3 in the event that the IT Health Check report identifies any vulnerabilities:

6.2.3.1 prepare a Vulnerability Correction Plan for Approval which sets out in respect of each such vulnerability:

6.2.3.1.1 how the vulnerability will be remedied;

6.2.3.1.2 the date by which the vulnerability will be remedied;

6.2.3.1.3 the tests which the Supplier shall perform or procure to be performed (which may, at the Authority's discretion, include a further IT Health Check) to confirm that the vulnerability has been remedied;

6.2.3.2 comply with the Vulnerability Correction Plan; and

6.2.3.3 conduct such further Security Tests as are required by the Vulnerability Correction Plan.

6.3 Security Tests shall be designed and implemented by the Supplier so as to minimise any adverse effect on the Services and the date, timing, content and conduct of Security Tests shall be agreed in advance with the Authority.

6.4 The Authority may send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Authority with the results of Security Tests (in a form to be Approved) as soon as practicable and in any event within 5 Working Days after completion of each Security Test.

6.5 Without prejudice to any other right of audit or access granted to the Authority pursuant to the Contract, the Authority and/or its authorised representatives, including any accreditor, may at any time to carry out Security Tests (including penetration tests) as it may deem necessary as part of any accreditation process and/or to verify the Supplier's compliance with the ISMS and the Security Plan:

6.5.1 upon giving reasonable notice to the Supplier where reasonably practicable to do so; and

6.5.2 without giving notice to the Supplier where, in the Authority's view, the provision of such notice may undermine the Security Tests to be carried out

and, where applicable, the Authority shall be granted access to the Supplier's premises for the purpose of undertaking the relevant Security Tests.

6.6 If the Authority carries out Security Tests in accordance with paragraphs 6.5.1 or 6.5.2, the Authority shall (unless there is any reason to withhold such information) notify the Supplier of the results of the Security Tests as soon as possible and in any event within 5 Working Days after completion of each Security Test.

6.7 If any Security Test carried out pursuant to paragraphs 6.1 or 6.4 reveals any:

6.7.1 vulnerabilities during any accreditation process, the Supplier shall track and resolve them effectively; and

6.7.2 actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Authority of any proposed changes to the ICT Environment (to the extent that this is under the control of the Supplier) and/or to the ISMS and/or to the Security Plan (and the implementation thereof) which the Supplier intends to make in order to correct such failure or weakness. Subject to Approval and paragraphs 4.3 and 4.4, the Supplier shall implement such changes to the ICT Environment (to the extent that this is under the control of the Supplier) and/or the ISMS and/or the Security Plan and repeat the relevant Security Tests in accordance with an Approved timetable or, otherwise, as soon as reasonably practicable.

6.8 If the Authority unreasonably withholds its approval to the implementation of any changes to the ICT Environment and/or to the ISMS and/or to the Security Plan proposed by the Supplier in accordance with paragraph 6.7, the Supplier is not in breach of the Contract to the extent that it can be shown that such breach:

6.8.1 has arisen as a direct result of the Authority unreasonably withholding Approval to the implementation of such proposed changes; and

6.8.2 would have been avoided had the Authority Approved the implementation of such proposed changes.

6.9 If a change to the ISMS or Security Plan is to address any non-compliance with ISO/IEC 27001:2013 requirements or equivalent, the Baseline Security Requirements or any obligations in the Contract, the Supplier shall implement such change at its own cost and expense.

6.10 If any repeat Security Test carried out pursuant to paragraph 6.7 reveals an actual or potential breach of security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default.

6.11 On each anniversary of the Commencement Date, the Supplier shall provide to the Authority a letter from the individual appointed or identified in accordance with paragraph 1.3 confirming that having made due and careful enquiry:

6.11.1 the Supplier has in the previous year carried out all Security Tests in accordance with this Schedule 6 and has complied with all procedures in relation to security matters required under the Contract; and

6.11.2 the Supplier is confident that its security and risk mitigation procedures in relation to Information Assets and Authority Data remain effective.

7. SECURITY AUDITS AND COMPLIANCE

7.1 The Authority and its authorised representatives may carry out security audits as it reasonably considers necessary in order to ensure that the ISMS is compliant with the principles and practices of ISO 27001: 2013 or equivalent (unless otherwise Approved), the requirements of this Schedule 6 and the Baseline Security Requirements.

7.2 If ISO/IEC 27001: 2013 certification or equivalent is provided; the ISMS shall be independently audited in accordance with ISO/IEC 27001: 2013 or equivalent. The Authority and its authorised representatives shall, where applicable, be granted access to the Supplier Sites and Sub-contractor premises for this purpose.

7.3 If, on the basis of evidence resulting from such audits, it is the Authority's reasonable opinion that ISMS is not compliant with any applicable principles and practices of ISO/IEC 27001: 2013 or equivalent, the requirements of this Schedule 6 and/or the Baseline Security Requirements is not being achieved by the Supplier, the Authority shall notify the Supplier of this and provide a reasonable period of time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) for the Supplier to implement any necessary remedy. If the Supplier does not ensure that the ISMS is compliant within this period of time, the Authority may obtain an independent audit of the ISMS to assess compliance (in whole or in part).

7.4 If, as a result of any such independent audit as described in paragraph 7.3 the Supplier is found to be non-compliant with any applicable principles and practices of ISO/IEC 27001:2013 or equivalent, the requirements of this Schedule 6 and/or the Baseline Security Requirements the Supplier shall, at its own cost, undertake those actions that are required in order to ensure that the ISMS is complaint and shall reimburse the Authority in full in respect of the costs obtaining such an audit.

8. SECURITY RISKS AND BREACHES

8.1 The Supplier shall use its reasonable endeavours to prevent any Breach of Security for any reason, including as a result of malicious, accidental or inadvertent behaviour.

8.2 If either Party becomes aware of a Breach of Security or an attempted Breach of Security it shall act in accordance with the agreed security incident management processes and incident response plans as set out in the ISMS.

8.3 Without prejudice to the security incident management processes and incident response plans set out in the ISMS and any requirements to report incidents in accordance with PSI 24/2014 if applicable, upon becoming aware of any Breach of Security or attempted Breach of Security, the Supplier shall:

8.3.1 immediately notify the Authority and take all reasonable steps (which shall include any action or changes reasonably required by the Authority) that are necessary to:

8.3.1.1 minimise the extent of actual or potential harm caused by any Breach of Security;

8.3.1.2 remedy any Breach of Security to the extent that is possible and protect the integrity of the ICT Environment (to the extent that this is within its control) and ISMS against any such Breach of Security or attempted Breach of Security;

8.3.1.3 mitigate against a Breach of Security or attempted Breach of Security; and

8.3.1.4 prevent a further Breach of Security or attempted Breach of Security in the future resulting from the same root cause failure;

8.3.2 provide to the Authority and/or the Computer Emergency Response Team for UK Government ("**GovCertUK**") or equivalent any data that is requested relating to the

Breach of Security or attempted Breach of Security within 2 Working Days of such request; and

8.3.3 as soon as reasonably practicable and, in any event, within 2 Working Days following the Breach of Security or attempted Breach of Security, provide to the Authority full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis if required by the Authority

and the Supplier recognises that the Authority may report significant actual or potential losses of Personal Data to the Information Commissioner or equivalent and to the Cabinet Office.

8.4 If any action is taken by the Supplier in response to a Breach of Security or attempted Breach of Security which occurred as a result of non-compliance of the ISMS with any ISO/IEC 27001: 2013 requirements or equivalent (as applicable), the Baseline Security Requirements and/or the requirements of this Schedule 6, any such action and change to the ISMS and/or Security Plan as a result shall be implemented at the Supplier's cost.

IT Environment

8.5 The Supplier shall ensure that the Supplier System:

8.5.1 functions in accordance with Good Industry Practice for protecting external connections to the internet;

8.5.2 functions in accordance with Good Industry Practice for protection from malicious code;

8.5.3 provides controls to securely manage (store and propagate) all cryptographic keys to prevent malicious entities and services gaining access to them, in line with the Authority's Cryptographic Policy as made available to the Supplier from time to time;

8.5.4 is patched (and all of its components are patched) in line with Good Industry Practice, any Authority patching policy currently in effect and notified to the Supplier and any Supplier patch policy that is agreed with the Authority; and

8.5.5 uses the latest versions of anti-virus definitions, firmware and software available from industry accepted anti-virus software vendors.

8.6 Notwithstanding paragraph 8.5, if a Breach of Security is detected in the ICT Environment, the Parties shall co-operate to reduce the effect of the Breach of Security and, if the Breach of Security causes loss of operational efficiency or loss or corruption of Information Assets and/or Authority Data, assist each other to mitigate any losses and to recover and restore such Information Assets and Authority Data.

8.7 All costs arising out of the actions taken by the Parties in compliance with paragraphs 8.2, 8.3 and 8.6 shall be borne by:

8.7.1 the Supplier if the Breach of Security originates from the defeat of the Supplier's security controls or Information Assets and/or Authority Data is lost or corrupted whilst under the control of the Supplier or its Sub-contractor; or

8.7.2 the Authority if the Breach of Security originates from the defeat of the Authority's security controls or Information Assets and/or Authority Data is lost or corrupted whilst under the control of the Authority

and each Party shall bear its own costs in all other cases.

9. VULNERABILITIES AND CORRECTIVE ACTION

9.1 The Parties acknowledge that from time to time vulnerabilities in the ICT Environment and ISMS will be discovered which, unless mitigated, will present an unacceptable risk to Information Assets and/or Authority Data.

9.2 The severity of any vulnerabilities shall be categorised by the Supplier as '*Critical*', '*Important*' and '*Other*' according to the agreed method in the ISMS and using any appropriate vulnerability scoring systems.

9.3 The Supplier shall procure the application of security patches to vulnerabilities categorised as '*Critical*' within 7 days of public release, vulnerabilities categorised as '*Important*' within 30 days of public release and vulnerabilities categorised as '*Other*' within 60 days of public release, except where:

9.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of the Services being provided, including where it resides in a software component which is not being used, provided that, where those vulnerabilities become exploitable, they are remedied by the Supplier within the timescales in paragraph 9.3;

9.3.2 the application of a security patch in respect of a vulnerability categorised as '*Critical*' or '*Important*' adversely affects the Supplier's ability to deliver the Services, in which case the Supplier shall be granted an extension to the timescales in paragraph 9.3 of 5 days, provided that the Supplier continues to follow any security patch test plan agreed with the Authority; or

9.3.3 the Authority agrees a different timescale after consultation with the Supplier in accordance with the processes defined in the ISMS.

9.4 The ISMS and the Security Plan shall include provision for the Supplier to upgrade software throughout the Term within 6 months of the release of the latest version unless:

9.4.1 upgrading such software reduces the level of mitigation for known threats, vulnerabilities or exploitation techniques, provided always that such software is upgraded by the Supplier within 12 months of release of the latest version; or

9.4.2 otherwise agreed with the Authority in writing.

9.5 The Supplier shall:

9.5.1 implement a mechanism for receiving, analysing and acting upon threat information provided by GovCertUK, or any other competent central Government Body;

9.5.2 ensure that the ICT Environment (to the extent that this is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

9.5.3 ensure that it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment (to the extent that this is within the control of the Supplier) by actively monitoring the threat landscape during the Term;

9.5.4 pro-actively scan the ICT Environment (to the extent that this is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS;

9.5.5 from the Commencement Date and within 5 Working Days of the end of each subsequent month during the Term provide a report to the Authority detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that this is within the control of the Supplier) and any elapsed time between the public release date of patches and either the time of application or, for outstanding vulnerabilities, the time of issue of such report;

9.5.6 propose interim mitigation measures in respect of any vulnerabilities in the ICT Environment (to the extent this is within the control of the Supplier) known to be exploitable where a security patch is not immediately available;

9.5.7 remove or disable any extraneous interfaces, services or capabilities that are no longer needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment to the extent this is within the control of the Supplier); and

9.5.8 inform the Authority when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the IT Environment (to the extent this is within the control of the Supplier) and provide initial indications of possible mitigations.

9.6 If the Supplier is unlikely to be able to mitigate any vulnerability within the timescales in paragraph 9.3, the Supplier shall notify the Authority immediately.

9.7 Any failure by the Supplier to comply with paragraph 9.3 shall constitute a material Default.

10. SUB-CONTRACTS

10.1 The Supplier shall ensure that all Sub-Contracts with Sub-Contractors who have access to Information Assets and/or Authority Data contain equivalent provisions in relation to information assurance and security that are no less onerous than those imposed on the Supplier under the Contract.

ANNEX 1 – BASELINE SECURITY REQUIREMENTS

1 Security Classifications and Controls

1.1 The Supplier shall, unless otherwise Approved in accordance with paragraph 6.2 of this Annexe 1, only have access to and handle Information Assets and Authority Data that are classified under the Government Security Classifications Scheme as OFFICIAL.

1.2 There may be a specific requirement for the Supplier in some instances on a limited 'need to know basis' to have access to and handle Information Assets and Authority Data that are classified as 'OFFICIAL-SENSITIVE.'

1.3 The Supplier shall apply the minimum security controls required for OFFICIAL information and OFFICIAL-SENSITIVE information as described in Cabinet Office guidance, currently at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf.

1.4 The Supplier shall be able to demonstrate to the Authority and any accreditor that it has taken into account the "Technical Controls Summary" for OFFICIAL (in the above guidance) in designing and implementing the security controls in the Supplier System, which shall be subject to assurance and accreditation to Government standards.

1.5 Additional controls may be required by the Authority and any accreditor where there are aspects of data aggregation.

2 End User Devices

2.1 Authority Data shall, wherever possible, be held and accessed on paper or in the ICT Environment on secure premises and not on removable media (including laptops, removable discs, CD-ROMs, USB memory sticks, PDAs and media card formats) without Approval. If Approval is sought to hold and access

data by other means, the Supplier shall consider the second-best option and third best option below and record the reasons why a particular approach should be adopted when seeking Approval:

2.1.1 second best option means: secure remote access so that data can be viewed or amended over the internet without being permanently stored on the remote device, using products meeting the FIPS 140-2 standard or equivalent, unless Approved;

2.1.2 third best option means: secure transfer of Authority Data to a remote device at a secure site on which it will be permanently stored, in which case the Authority Data and any links to it shall be protected at least to the FIPS 140-2 standard or equivalent, unless otherwise Approved, and noting that protectively marked Authority Data must not be stored on privately owned devices unless they are protected in this way.

2.2 The right to transfer Authority Data to a remote device should be carefully considered and strictly limited to ensure that it is only provided where absolutely necessary and shall be subject to monitoring by the Supplier and Authority.

2.3 Unless otherwise Approved, when Authority Data resides on a mobile, removable or physically uncontrolled device, it shall be:

2.3.1 the minimum amount that is necessary to achieve the intended purpose and should be anonymised if possible;

2.3.2 stored in an encrypted form meeting the FIPS 140-2 standard or equivalent and using a product or system component which has been formally assured through a recognised certification process of CESG to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("**CPA**") or equivalent, unless otherwise Approved;

2.3.3 protected by an authentication mechanism, such as a password; and

2.3.4 have up to date software patches, anti-virus software and other applicable security controls to meet the requirements of this Schedule 6.

2.4 Devices used to access or manage Authority Data shall be under the management authority of the Supplier and have a minimum set of security policy configurations enforced. Unless otherwise Approved, all Supplier devices shall satisfy the security requirements set out in the CESG End User Devices Platform Security Guidance ("**CESG Guidance**") (https://www.gov.uk/government/collections/end-user-devices-security-guidance--2) or equivalent.

2.5 Where the CESG Guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Authority and a joint decision shall be taken on whether the residual risks are acceptable. If the Supplier wishes to deviate from the CESG Guidance, this should be agreed in writing with the Authority on a case by case basis.

3 Data Storage, Processing, Management, Transfer and Destruction

3.1 The Parties recognise the need for Authority Data to be safeguarded and for compliance with the Data Protection Legislation. To that end, the Supplier shall inform the Authority the location within the United Kingdom where Authority Data is stored, processed and managed. The import and export of Authority Data from the Supplier System must be strictly controlled and recorded.

3.2 The Supplier shall inform the Authority of any changes to the location within the United Kingdom where Authority Data is stored, processed and managed and shall not transmit, store, process or manage Authority Data outside of the United Kingdom without Approval which shall not be unreasonably withheld or delayed provided that the transmission, storage, processing and management of Authority Data offshore is within:

3.2.1 the European Economic Area ("**EEA**"); or

3.2.2 another country or territory outside the EEA if that country or territory ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into which have been defined as adequate by the European commission.

3.3 The Supplier System shall support the requirement of the Authority to comply with Government policy and Cabinet Office guidance on Offshoring, currently set out at:

https://ogsirooffshoring.zendesk.com/hc/en-us/articles/203107991-HMG-sOffshoring-Policy

by assessing, as required, any additional security risks associated with the storage, processing and/or transmission of any data and/or information offshore, including by an offshore Supplier (which may include the use of 'landed resources'), taking account of European Union requirements to confirm the 'adequacy' of protection of Personal Data in the countries where storage, processing and/or transmission occurs. No element of the Supplier System may be off-shored without Approval.

3.4 The Supplier shall ensure that the Supplier System provides internal processing controls between security domains to prevent the unauthorised high domain exporting of Authority Data to the low domain if there is a requirement to pass data between different security domains.

3.5 The Supplier shall ensure that any electronic transfer of Authority Data:

3.5.1 protects the confidentiality of the Authority during transfer through encryption suitable for the impact level of the data;

3.5.2 maintains the integrity of the Authority Data during both transfer and loading into the receiving system through suitable technical controls for the impact level of the data; and

3.5.3 prevents the repudiation of receipt through accounting and auditing.

3.6 The Supplier shall:

3.6.1 protect Authority Data, including Personal Data, whose release or loss could cause harm or distress to individuals and ensure that this is handled as if it were confidential while it is stored and/or processed;

3.6.2 ensure that any OFFICIAL-SENSITIVE information, including Personal Data is encrypted in transit and when at rest when stored away from the Supplier's controlled environment;

3.6.3 on demand, provide the Authority with all Authority Data in an agreed open format;

3.6.4 have documented processes to guarantee availability of Authority Data if it ceases to trade;

3.6.5 securely destroy all media that has held Authority Data at the end of life of that media in accordance with any requirements in the Contract and, in the absence of any such requirements, in accordance with Good Industry Practice;

3.6.6 securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority;

3.6.7 ensure that all material used for storage of Confidential Information is subject to controlled disposal and the Supplier shall:

3.6.7.1 destroy paper records containing Personal Data by incineration, pulping or shredding so that reconstruction is unlikely; and

3.6.7.2 dispose of electronic media that was used for the processing or storage of Personal Data through secure destruction, overwriting, erasure or degaussing for re-use.

4 Networking

4.1 Any Authority Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under CPA or through the use of Public Sector Network ("**PSN**") compliant encrypted networking services or equivalent unless none are available in which case the Supplier shall agree the solution with the Authority.

4.2 The Supplier shall ensure that the configuration and use of all networking equipment in relation to the provision of the Services, including equipment that is located in secure physical locations, shall be at least compliant with Good Industry Practice.

4.3 The Supplier shall ensure that the ICT Environment (to the extent this is within the control of the Supplier) contains controls to maintain separation between the PSN and internet connections if used.

5 Security Architectures

5.1 When designing and configuring the ICT Environment (to the extent that this is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or those with a CESG Certified Professional certification (http://www.cesg.gov.uk/awarenesstraining/IA-certification/Pages/index.aspx) or equivalent for all bespoke or complex components.

5.2 The Supplier shall provide to the Authority and any accreditor sufficient design documentation detailing the security architecture of the ICT Environment and data transfer mechanism to support the Authority's and any accreditor's assurance that this is appropriate, secure and compliant with the Authority's requirements.

5.3 The Supplier shall apply the *'principle of least privilege'* (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of the ICT Environment used for the storage, processing and management of Authority Data. Users should only be granted the minimum necessary permissions to access Information Assets and Authority Data and must be automatically logged out of the Supplier System if an account or session is inactive for more than 15 minutes.

6 Digital Continuity

The Supplier shall ensure that each Information Asset is held in an appropriate format that is capable of being updated from time to time to enable the Information Asset to be retrieved, accessed, used and transferred to the Authority, including in accordance with any information handling procedures set out in PSI 24/2014 (Information Assurance) if applicable.

7 Personnel Vetting and Security

7.1 All Staff shall be subject to pre-employment checks that include, as a minimum, their employment history for at least the last 3 years, identity, unspent criminal convictions and right to work (including nationality and immigration status) and shall be vetted in accordance with:

7.1.1 the BPSS or BS7858 or equivalent; and

7.1.2 PSI 07/2014, if applicable, based on their level of access to Information Assets and/or Authority Data.

7.2 If the Authority agrees that it is necessary for any Staff to have logical or physical access to Information Assets and/or Authority Data classified at a higher level than OFFICIAL (such as that requiring '*SC*' clearance), the Supplier shall obtain the specific Government clearances that are required for access to such Information Assets and/or Authority Data.

7.3 The Supplier shall prevent Staff who are unable to obtain the required security clearances from accessing Information Assets and/or Authority Data and/or the ICT Environment used to store, process and/or manage such Information Assets or Authority Data.

7.4 The Supplier shall procure that all Staff comply with the Security Policy Framework and principles, obligations and policy priorities stated therein, including requirements to manage and report all security risks in relation to the provision of the Services.

7.5 The Supplier shall ensure that Staff who can access Information Assets and/or Authority Data and/or the ICT Environment are aware of their responsibilities when handling such information and data and undergo regular training on secure information management principles. Unless otherwise Approved, this training must be undertaken annually.

7.6 If the Supplier grants Staff access to Information Assets and/or Authority Data, those individuals shall be granted only such levels of access and permissions that are necessary for them to carry out their duties. Once Staff no longer require such levels of access or permissions or leave the organisation, their access rights shall be changed or revoked (as applicable) within one Working Day.

8 Identity, Authentication and Access Control

8.1 The Supplier shall operate a robust role-based access control regime, including network controls, to ensure all users and administrators of and those maintaining the ICT Environment are uniquely identified and authenticated when accessing or administering the ICT Environment to prevent unauthorised users from gaining access to Information Assets and/or Authority Data. Applying the '*principle of least privilege*', users and administrators and those responsible for maintenance shall be allowed access only to those parts of the ICT Environment they require. The Supplier shall retain an audit record of accesses and users and disclose this to the Authority upon request.

8.2 The Supplier shall ensure that Staff who use the Authority System actively confirm annually their acceptance of the Authority's acceptable use policy.

9 Physical Media

9.1 The Supplier shall ensure that all:

9.1.1 OFFICIAL information is afforded physical protection from internal, external and environmental threats commensurate with the value to the Authority of that information;

9.1.2 physical components of the Supplier System are kept in secure accommodation which conforms to the Security Policy Framework and CESG standards and guidance or equivalent;

9.1.3 physical media holding OFFICIAL information is handled in accordance with the Security Policy Framework and CESG standards and guidance or equivalent; and

9.1.4 Information Assets and Authority Data held on paper are:

9.1.4.1 kept secure at all times, locked away when not in use on the premises on which they are held and secured and are segregated if the Supplier is co-locating with the Authority; and

9.1.4.2 only transferred by an approved secure form of transfer with confirmation of receipt obtained.

10 Audit and Monitoring

10.1 The Supplier shall implement effective monitoring of its information assurance and security obligations in accordance with Government standards and where appropriate, in accordance with CESG Good Practice Guide 13 – Protective Monitoring or equivalent.

10.2 The Supplier shall collect audit records which relate to security events in the ICT Environment (where this is within the control of the Supplier), including those that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness, such Supplier audit records shall include:

10.2.1 logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent it is within the control of the Supplier). To the extent, the design of the ICT Environment allows, such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers;

10.2.2 regular reports and alerts giving details of access by users of the ICT Environment (to the extent that it is within the control of the Supplier) to enable the identification of changing access trends any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data; and

10.2.3 security events generated in the ICT Environment (to the extent it is within the control of the Supplier) including account logon and logoff events, start and end of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

10.3 The Parties shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

10.4 The Supplier shall retain audit records collected in compliance with paragraph 10.1 for at least 6 months.

SCHEDULE 7 - PRISONS

ACCESS TO PRISONS

1 If Staff are required to have a pass for admission to an Authority Premises which is a prison, (a "**Prison**") the Authority shall, subject to satisfactory completion of approval procedures, arrange for passes to be issued. Any member of the Staff who cannot produce a proper pass when required to do so by any member of the Authority's personnel, or who contravenes any conditions on the basis of which a pass was issued, may be refused admission to a Prison or be required to leave a Prison if already there.

2 Staff shall promptly return any pass if at any time the Authority so requires or if the person to whom the pass was issued ceases to be involved in the performance of the Services. The Supplier shall promptly return all passes on expiry or termination of the Contract.

3 Staff attending a Prison may be subject to search at any time. Strip searches shall be carried out only on the specific authority of the Authority under the same rules and conditions applying to the Authority's personnel. The Supplier is referred to Rule 71 of Part IV of the Prison Rules 1999 as amended by the Prison (Amendment) Rules 2005 and Rule 75 of Part IV of the Young Offender Institution Rules 2000 as amended by the Young Offender Institution (Amendment) Rules 2005.

4 Searches shall be conducted only on the specific authority of the Authority under the same rules and conditions applying to the Authority's personnel and/or visitors. The Supplier is referred to Section 8 of the Prison Act 1952, Rule 64 of the Prison Rules 1999 and PSI 07/2016.

SECURITY

5 Whilst at Prisons Staff shall comply with all security measures implemented by the Authority in respect of staff and other persons attending Prisons. The Authority shall provide copies of its written security procedures to Staff on request. The Supplier and all Staff are prohibited from taking any photographs at Prisons unless they have Approval and the Authority's representative is present so as to have full control over the subject matter of each photograph to be taken. No such photograph shall be published or otherwise circulated without Approval.

6 The Authority may search vehicles used by the Supplier or Staff at Prisons.

7 The Supplier and Staff shall co-operate with any investigation relating to security which is carried out by the Authority or by any person who is responsible for security matters on the Authority's behalf, and when required by the Authority shall:

7.1 take all reasonable measures to make available for interview by the Authority any members of Staff identified by the Authority, or by a person who is responsible for security matters, for the purposes of the investigation. Staff may be accompanied by and be advised or represented by another person whose attendance at the interview is acceptable to the Authority; and

7.2 subject to any legal restriction on their disclosure, provide all documents, records or other material of any kind and in whatever form which may be reasonably required by the Authority, or by a person who is responsible for security matters on the Authority's behalf, for the purposes of investigation as long as the provision of that material does not prevent the Supplier from performing the Services. The Authority may retain any such material for use in connection with the investigation and, as far as possible, may provide the Supplier with a copy of any material retained.

OFFENCES AND AUTHORISATION

8 In providing the Services the Supplier shall comply with PSI 10/2012 (Conveyance and Possession of Prohibited Items and Other Related Offences) and other applicable provisions relating to security as published by the Authority from time to time.

9 Nothing in the Contract is deemed to provide any "authorisation" to the Supplier in respect of any provision of the Prison Act 1952, Offender Management Act 2007, Crime and Security Act 2010, Serious Crime Act 2015 or other relevant legislation.

SCHEDULE 8 – STATUTORY OBLIGATIONS AND CORPORATE SOCIAL RESPONSIBILITY

1 What the Authority expects from the Supplier

1.1 In February 2019, Her Majesty's Government published version 2 of a Supplier Code of Conduct (the "**Code**") setting out the standards and behaviours expected of suppliers who work with government. The Code can be found online at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779660/20190220-Supplier_Code_of_Conduct.pdf

1.2 The Authority expects the Supplier and its Sub-Contractors to comply with their legal obligations, in particular those set out in Part 1 of this Schedule 8, and to meet the standards set out in the Code as a minimum. The Authority also expects the Supplier and its Sub-Contractors to use reasonable endeavours to comply with the standards set out in Part 2 of this Schedule 8.

PART 1 Statutory Obligations

2 Equality and Accessibility

2.1 The Supplier shall:

(a) perform its obligations under the Contract in accordance with:

i) all applicable equality Law (whether in relation to race, sex, gender reassignment, age, disability, sexual orientation, religion or belief, pregnancy maternity or otherwise);

ii) the Authority's equality, diversity and inclusion policy as given to the Supplier from time to time;

iii) any other requirements and instructions which the Authority reasonably imposes regarding any equality obligations imposed on the Authority at any time under applicable equality law; and

(b) take all necessary steps and inform the Authority of the steps taken to prevent unlawful discrimination designated as such by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation).

3 Modern Slavery

3.1 The Supplier shall, and procure that each of its Sub-Contractors shall, comply with:

(a) the MSA; and

(b) the Authority's anti-slavery policy as provided to the Supplier from time to time ("**Anti-slavery Policy**").

3.2 The Supplier shall:

(a) implement due diligence procedures for its Sub-Contractors and other participants in its supply chains, to ensure that there is no slavery or trafficking in its supply chains;

(b) respond promptly to all slavery and trafficking due diligence questionnaires issued to it by the Authority from time to time and shall ensure that its responses to all such questionnaires are complete and accurate;

(c) prepare and deliver to the Authority each year, an annual slavery and trafficking report setting out the steps it has taken to ensure that slavery and trafficking is not taking place in any of its supply chains or in any part of its business;

(d) maintain a complete set of records to trace the supply chain of all Services provided to the Authority regarding the Contract;

(e) report the discovery or suspicion of any slavery or trafficking by it or its Sub-Contractors to the Authority and to the Modern Slavery Helpline; and

(f) implement a system of training for its employees to ensure compliance with the MSA.

3.3 The Supplier represents, warrants and undertakes throughout the Term that:

(a) it conducts its business in a manner consistent with all applicable laws, regulations and codes including the MSA and all analogous legislation in place in any part of the world;

(b) its responses to all slavery and trafficking due diligence questionnaires issued to it by the Authority from time to time are complete and accurate; and

(c) neither the Supplier nor any of its Sub-Contractors, nor any other persons associated with it:

i) has been convicted of any offence involving slavery and trafficking; or

ii) has been or is the subject of any investigation, inquiry or enforcement proceedings by any governmental, administrative or regulatory body regarding any offence regarding slavery and trafficking.

3.4 The Supplier shall notify the Authority as soon as it becomes aware of:

(a) any breach, or potential breach, of the Anti-Slavery Policy; or

(b) any actual or suspected slavery or trafficking in a supply chain which relates to the Contract.

3.5 If the Supplier notifies the Authority pursuant to paragraph 3.4 of this Schedule 8, it shall respond promptly to the Authority's enquiries, co-operate with any investigation, and allow the Authority to audit any books, records and/or any other relevant documentation in accordance with the Contract.

3.6 If the Supplier is in Default under paragraphs 3.2 or 3.3 of this Schedule 8 the Authority may by notice:

(a) require the Supplier to remove from performance of the Contract any Sub-Contractor, Staff or other persons associated with it whose acts or omissions have caused the Default; or

(b) immediately terminate the Contract.

4 Income Security

4.1 The Supplier shall:

(a) ensure that all pay and benefits paid for a standard working week meet, at least, national legal standards in the country of employment;

(b) provide all Staff with written and readily understandable information about their employment conditions in respect of pay before they enter employment and about their pay for the pay period concerned each time that they are paid;

(c) not make deductions from pay:

(i) as a disciplinary measure;

(ii) except where permitted by Law and the terms of the employment contract; and

(iii) without express permission of the person concerned

(d) record all disciplinary measures taken against Staff.

5 Working Hours

5.1 The Supplier shall ensure that:

(a) the working hours of Staff comply with the Law, and any collective agreements;

(b) the working hours of Staff, excluding overtime, is defined by contract, do not exceed 48 hours per week unless the individual has agreed in writing, and that any such agreement is in accordance with the Law;

(c) overtime is used responsibly, considering:

(i) the extent;

(ii) frequency; and

(iii) hours worked;

(d) the total hours worked in any seven-day period shall not exceed 60 hours, except where covered by paragraph 5.1 (e);

(e) working hours do not exceed 60 hours in any seven-day period unless:

(i) it is allowed by Law;

(ii) it is allowed by a collective agreement freely negotiated with a worker's organisation representing a significant portion of the workforce;

(iii) appropriate safeguards are taken to protect the workers' health and safety; and

(iv) the Supplier can demonstrate that exceptional circumstances apply such as during unexpected production peaks, accidents or emergencies;

(f) all Supplier Staff are provided with at least:

(i) 1 day off in every 7-day period; or

(ii) where allowed by Law, 2 days off in every 14-day period.

6 Right to Work

6.1 The Supplier shall:

(a) ensure that all Staff, are employed on the condition that they are permitted to work in the UK, and;

(b) notify the authority immediately if an employee is not permitted to work in the UK.

7 Health and Safety

7.1 The Supplier shall perform its obligations under the Contract in accordance with:

(a) all applicable Law regarding health and safety; and

(b) the Authority's Health and Safety Policy while at the Authority's Premises.

7.2 Each Party shall notify the other as soon as practicable of any health and safety incidents or material health and safety hazards at the Authority's Premises of which it becomes aware and which relate to or arise in connection with the performance of the Contract. The Supplier shall instruct Staff to adopt any necessary safety measures in order to manage the risk.

8. Welsh Language Requirements

8.1 The Supplier shall comply with the Welsh Language Act 1993 and the Welsh Language Scheme as if it were the Authority to the extent that the same relate to the provision of the Services.

9 Fraud and Bribery

9.1 The Supplier represents and warrants that neither it, nor to the best of its knowledge any Staff, have at any time prior to the Commencement Date:

(a) 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

(b) 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.

9.2 The Supplier shall not during the Term:

(a) commit a Prohibited Act; and/or

(b) do or suffer anything to be done which would cause the Authority or any of its 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.

9.3 The Supplier shall, during the Term:

(a) establish, maintain and enforce, and require that its Sub-Contractors 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;

(b) have in place reasonable prevention measures (as defined in section 45(3) and 46(4) of the Criminal Finance Act 2017) to ensure that Associated Persons of the Supplier do not commit tax evasion facilitation offences as defined under that Act;

(c) keep appropriate records of its compliance with its obligations under paragraph 9.3 (a) and 9.3 (b) and make such records available to the Authority on request; and

(d) take account of any guidance about preventing facilitation of tax evasion offences which may be published and updated in accordance with section 47 of the Criminal Finances Act 2017

9.4 The Supplier shall immediately notify the Authority in writing if it becomes aware of any breach of paragraphs 9.1 and/or 9.2, or has reason to believe that it has or any of the Staff have:

(a) been subject to an investigation or prosecution which relates to an alleged Prohibited Act;

(b) 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; and/or

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

9.5 If the Supplier notifies the Authority pursuant to paragraph 9.4, the Supplier shall respond promptly to the Authority's enquiries, co-operate with any investigation, and allow the Authority to Audit any books, records and/or any other relevant documentation.

9.6 If the Supplier is in Default under paragraphs 9.1 and/or 9.2, the Authority may by notice:

(a) require the Supplier to remove from performance of the Contract any Staff whose acts or omissions have caused the Default; or

(b) immediately terminate the Contract.

9.7 Any notice served by the Authority under paragraph 9.6 shall specify the nature of the Prohibited Act, the identity of the party who the Authority believes has committed the Prohibited Act and the action that the Authority has taken (including, where relevant, the date on which the Contract terminates).

PART 2 Corporate Social Responsibility

10 Zero Hours Contracts

10.1 Any reference to zero hours contracts, for the purposes of this Contract, means as they relate to employees or workers and not those who are genuinely self-employed and undertaking work on a zero hours arrangement.

10.2 When offering zero hours contracts, the Supplier shall consider and be clear in its communications with its employees and workers about:

(a) whether an individual is an employee or worker and what statutory and other rights they have;

(b) the process by which work will be offered and assurance that they are not obliged to accept work on every occasion; and

(c) how the individual's contract will terminate, for example, at the end of each work task or with notice given by either party.

11 Sustainability

11.1 The Supplier shall:

(a) comply with the applicable Government Buying Standards;

(b) provide, from time to time, in a format reasonably required by the Authority, reports on the environmental effects of providing the Goods and Services;

(c) maintain ISO 14001 or BS 8555 or an equivalent standard intended to manage its environmental responsibilities; and

(b) perform its obligations under the Contract in a way that:

(i) supports the Authority's achievement of the Greening Government Commitments;
(ii) conserves energy, water, wood, paper and other resources;

(iii) reduces waste and avoids the use of ozone depleting substances; and

(iv) minimises the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment.

SCHEDULE 9 – DATA PROCESSING

1. The contact details of the Authority's Data Protection Officer are: Redacted Under FOIA Section 40

2. The contact details of the Supplier's Data Protection Officer are: Redacted Under FOIA Section 40

3. The Supplier shall comply with any further written instructions with respect to processing by the Authority.

4. Any such further instructions shall be incorporated into this Schedule 9.

Part A – Offender Personal Data

Description	Details
Subject matter of the processing	Any data produced or processed by virtue of the delivery of the Services under this contract. Specifically, the supplier will receive a range of referral details about offenders in order to consider residential placement wherein rehabilitative and tailored support packages will be delivered. Following the referral assessment and if placement is agreed the supplier will utilise the referral data to inform offender support, rehabilitation and risk management. The processing need is therefore to ensure that the Supplier can appropriately determine a rehabilitative and risk management framework to effectively deliver the contractual service safely and effectively.
Duration of the processing	Processing of Offender Personal Data is for the Term of this Contract; from Service Commencement until the Expiry Date or Termination Date, whichever falls earlier.
Nature and purposes of the processing	The purpose of the processing is, as per the contract; to provide accommodation and support services to offenders, as referred to the Supplier by the Authority The nature of the processing under this contract includes but is not limited to processing referrals to the service, case management, delivering purposeful interventions, risk management referrals to other agencies, statutory reporting, collection, recording, organization, structuring, storage, adaption, alteration, retrieval, consultation, use of, disclosure, transmission, dissemination or otherwise, making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) or Personal Data for the purpose of delivering the Services under this Contract.

Type of Personal Data being Processed	As per the referral form, including: • Name • DOB • Unique identification number • Establishment address and information (eg room number) • Current/previous accommodation address • Rent/housing arrears information • National insurance number • Offence information – including possible previous conviction information and licence information • Telephone numbers • Educational information (including SEN where relevant) • Risk assessment, social work reports, Pre Sentence /Parole Reports NPS records, case records and incident reports • Healthcare records • Substance misuse history • Images • Ethnicity • Religious belief • Sexual orientation • Gender identity • Disability • Legal status (e.g. remanded, convicted or awaiting sentence) • Release/sentence dates • LAC status • Parental status • Preferred communication • Responsible Local Authority • Personal testimony • Voice Recordings (subject to security clearance) • Armed forces service history
Categories of Data Subject	Referral group only – offenders referred to the Supplier by the Authority.
Plan for return and destruction of the data once the processing is complete Unless requirement under Law to preserve that type of data	Offender Personal Data is returned or destroyed according to the following timescales: a) **Referral data**: Offender Personal Data received from the Authority on referral is retained by the Supplier for the duration of the offender's stay after which it is deleted. For referrals that are not accepted into the services the Supplier deletes the Offender Personal Data within 6 months of initial referral.

	The Supplier will manage a system whereby they are able to identify rejected referrals which have reached the retention period limit, at which point the documents will be destroyed. b) **Ongoing case management data (including all Care Plans):** All Offender Personal Data created by the Supplier during the course of the Contract is retained for 6 years after the offender's departure. The Supplier will manage a system whereby they are able to identify archived case management data that has reached the retention period limit, at which point the documents will be destroyed.

Part B – Authority Data

Description	Details
Subject matter of the processing	Any data produced or processed by virtue of the delivery of the Services under this contract, that is not considered Offender Personal Data as outlined above in Part A but required to ensure the Supplier can appropriately deliver its Services under Contract.
Duration of the processing	Processing of Authority Data is for the Term of this Contract; from Service Commencement until the Expiry Date or Termination Date, whichever falls earlier.
Nature and purposes of the processing	The purpose of the processing is, as per the contract; to provide accommodation and support services to offenders, as referred to the Supplier by the Authority. The nature of the processing under this contract includes but is not limited to processing referrals to the service, case management, delivering purposeful interventions, risk management referrals to other agencies, statutory reporting, collection, recording, organization, structuring, storage, adaption, alteration, retrieval, consultation, use of, disclosure, transmission, dissemination or otherwise, making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) or Personal Data for the purpose of delivering the Services under this Contract.
Type of Personal Data being Processed	This could include personal data relating to Authority staff or other professionals, processed in the delivery of services and is not individual Offender Personal Data. A reason for such processing could be in compliance with general communication obligations under the contract, or potential enforcement or incident management scenarios involving individuals other than the offender. This could include: • Name • DOB • Work address • Telephone numbers

	• Personal or professional email addresses or other contact information • Security information (finger prints, CCTV footage etc) • Ethnicity • Religious belief • Sexual orientation • Gender identity • Disability • Personal testimony • Voice Recordings
Categories of Data Subject	Authority staff, other professionals or individuals processed in the delivery of services in relation to the case management of a referred offender.
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	Such personal data created or processed by the Supplier during the course of the Contract is retained for 6 years after contract expiry. The Supplier will manage a system whereby they are able to identify such archived data that has reached the retention period limit, at which point the documents will be destroyed.

Part C – Staff Personal Data

Description	Details
Subject matter of the processing	Any Staff Personal Data processed by the Authority by virtue of the delivery of the Services under this contract, that is not considered Offender Personal Data as outlined above in Part A or Authority Data as at part B above.
Duration of the processing	Processing of Staff Personal Data is for the Term of this Contract; from Service Commencement until the Expiry Date or Termination Date, whichever falls earlier.
Nature and purposes of the processing	The purpose of the Authority processing Supplier Staff Personal Data would be as per the contract and may involve the Authority exercising their rights of assurance and governance of the Contract. The nature of the processing under this contract includes but is not limited to, processing Supplier Staff Personal Data when reviewing vetting information, responding to PQs or FOIs, investigating incidents or contractual compliance issues, statutory reporting, collection, recording, organization, structuring, storage, adaption, alteration, retrieval, consultation, use of, disclosure, transmission, dissemination or otherwise, making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) or Personal Data for the purpose of assuring and managing the delivery of Services under this Contract.

Type of Personal Data being Processed	This could include Personal Data relating to Supplier Staff processed in the delivery of services and is not individual Offender Personal Data. This could include: • Name • DOB • Current/previous accommodation address • National insurance number • Telephone numbers • Healthcare records • Substance misuse history • Images • Ethnicity • Religious belief • Sexual orientation • Gender identity • Disability • Parental status • Preferred communication • Personal testimony • Voice Recordings (subject to security clearance) • Armed forces service history • Security information (finger prints, CCTV footage etc)
Categories of Data Subject	Supplier Staff involved in the delivery of services under this Contract.
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	Such personal data processed by the Authority during the course of the Contract is retained for 6 years after contract expiry.

SCHEDULE 10 – BUSINESS CONTINUITY PLAN

1.1 The Supplier shall develop, implement and maintain a Business Continuity Plan to apply during the Contract term (and after the end of the term as applicable) which will be approved by the Authority, tested, periodically updated and audited in accordance with this Schedule.

1.2 Within 30 days of the Commencement Date the Supplier will deliver to the Authority for approval its proposed final Business Continuity Plan, which will be based on the HMPPS Business Continuity Policy Framework found at Annex 1 to this Schedule. This document is to be read as if each reference to "NPS" applies equally to the Supplier.

1.3 If the Business Continuity Plan is approved by the Authority it will be adopted immediately. If it is not approved by the Authority the Supplier shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit to the Authority for approval. The Parties will use all reasonable endeavours to ensure that the approval 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 Authority. If the Authority does not approve the Business Continuity Plan following its resubmission, the matter will be resolved in accordance with clause I1 (Dispute Resolution). No approval to be given by the Authority pursuant to this paragraph 1.3 may be unreasonably withheld or delayed. Any failure to approve the Business Continuity Plan on the grounds that it does not comply with the requirements set out in paragraphs 1.1 to 1.3 shall be deemed to be reasonable.

1.4 The Business Continuity Plan shall, as a minimum:

(a) shall adhere to the principles contained in the HMPPS Business Continuity Policy Framework; and

(b) be drafted in the Business Continuity Plan template applicable to NPS.

2. TESTING

2.1 The Supplier shall, at no cost to the Authority, conduct a test of the Business Continuity Plan on an annual basis and on such further occasions as may reasonably be required by the Authority. The scope of such testing shall be agreed between the Parties.

2.2 The Supplier shall provide the Authority with a written report summarising the results of all tests carried out pursuant to paragraph 2.1, any failures of the Plan and any remedial action which the Supplier has taken or intends to take (which may include improvements to the Plan). The Authority may make

recommendations of remedial action and the Supplier shall implement such as soon as practically possible at no cost to the Authority.

3. INVOKING THE BUSINESS CONTINUITY PLAN

3.1 If an event occurs which, in the reasonable opinion of the Authority, constitutes an emergency or disaster affecting the Supplier's ability to perform the Services, the Supplier shall:

(a) immediately notify the Authority of the full details of the event and its anticipated impact on the Supplier's ability to perform its obligations under the Contract; and

(b) as soon as reasonably practicable but within a maximum of 6 hours:

(i) implement the Business Continuity Plan; and

(ii) agree with the Authority the steps that it will take to address and mitigate the event with a view to ensuring minimum disruption to the Services.

ANNEX 1

HMPPS-business-continuity-policy-framewc

IN WITNESS of which the Contract is duly executed by the Parties on the date which appears at the head of page 1.

SIGNED for and on behalf of the Secretary of State for Justice:

Signature:

Name (block capitals):

Position:

Date:

SIGNED for and on behalf of Redacted Under FOIA Section 40 :

Signature:

Name (block capitals):

Position: Chief Executive Officer

Date:

Signature:

Name (block capitals):

Position: Chair of Trustees

Date