

Date: [Redacted]

A Contract for Services

between

The Lord Chancellor

and

Advantis Credit Limited

CONTENTS

A1	Definitions and Interpretation	1
A2	Authority Obligations	16
A3	Supplier's Status	16
A4	Mistakes in Information	16
A5	Term	16
A6	Contract Management	17
B1	Basis of the Contract	17
B2	Delivery of the Services	17
B3	Equipment	18
B4	Key Personnel	19
B5	Staff	20
B6	Due Diligence	20
B7	Licence to Occupy	20
B8	Property	21
B9	Offers of Employment	22
B10	Employment	22
B11	Welsh Language Requirements	24
C1	Payment and VAT	24
C2	Recovery of Sums Due	27
C3	Price During Extension	27
D1	His Majesty's Government's Supplier Code of Conduct	27
D2	Fraud and Bribery	28
D3	Equality and Accessibility	29
D4	Health and Safety	30
D5	Modern Slavery Act	30
D6	Income Security	32
D7	Working Hours	32
D8	Right to Work	33
D9	Corporate Social Responsibility	33
E1	Authority Data	34
E2	Data Protection and Privacy	35
E3	Official Secrets Acts and Finance Act	40
E4	Confidential Information	40
E5	Freedom of Information	42
E6	Publicity, Media and Official Enquiries	43
E7	Intellectual Property Rights	43
E8	Audit	45
E9	Tax Compliance	47
F1	Performance Review	47
F2	Rectification Plan Process	48
F3	Enhanced Monitoring	50
F4	Remedies	51
F5	Transfer and Sub-Contracting	52
F6	Change	55

F7	MTR Change	56
G1	Liability, Indemnity and Insurance	56
G2	Warranties and Representations	58
H1	Insolvency and Change of Control	60
H2	Termination on Default	62
H3	Termination on Notice	63
H4	Other Termination Grounds	63
H5	Consequences of Expiry or Termination	64
H6	Disruption	64
H7	Recovery	65
H8	Retendering and Handover	65
H9	Exit Management	66
H10	Knowledge Retention	68
H11	Financial Distress	68
I1	Dispute Resolution	68
I2	Force Majeure	70
I3	Notices and Communications	71
I4	Conflicts of Interest	72
I5	Rights of Third Parties	72
I6	Remedies Cumulative	73
I7	Waiver	73
I8	Severability	73
I9	Entire Agreement	73
I10	Change of Law	73
I11	Counterparts	74
I12	Governing Law and Jurisdiction	74

Schedules

1. Specification
2. Pricing and Payment
3. Supplier Solution
4. Commercially Sensitive Information
5. Supplier and Third Party Software
6. Information Assurance and Security
7. Key Personnel
8. Performance, Management Information and Reporting
9. Business Continuity and Disaster Recovery
10. Data Processing
11. Approved Sub-Contractors
12. Change Control Forms
13. Governance and Contract Management
14. Policies and Standards
15. Implementation Plan
16. Exit Management
17. Deed of Guarantee and Indemnity
18. Financial Distress
19. Deed of Trust

This Contract is dated:

PARTIES:

- (1) THE LORD CHANCELLOR, acting as part of the Crown of 102 Petty France, London, SW1H 9AJ (the “**Authority**”);

AND

- (2) Advantis Credit Limited with registered company number 05223252 whose registered office is Floor 9 Peninsular House, 30-36 Monument Street, London, England, EC3R 8LJ (the “**Supplier**”);

(each a “**Party**” and together the “**Parties**”).

WHEREAS

- A. The Authority requires a debt collection and enforcement services supplier to deliver debt collection and enforcement services across England and Wales.
- B. The Supplier will be responsible for the collection of legal aid contributions (as and where appropriate) from individual recipients of legal aid and for pursuing appropriate enforcement action and associated case management activity. Collected payments will be paid to the Legal Aid Agency (the “**LAA**”) and Enforcement Costs (defined below) charged back to individual debtors where appropriate.
- C. The administration of legal aid and the operational management of this Contract will be the responsibility of the LAA on behalf of the Lord Chancellor.
- D. The Services will be delivered by Advantis Credit Limited (company number 05223252) for and on behalf of the Supplier. Advantis Credit Limited are a wholly owned subsidiary of the Supplier.
- E. The Supplier remains responsible for all provisions under the Contract.
- F. The Guarantee has been entered into on or about the date of this Contract.

NOW IT IS HEREBY AGREED:

A GENERAL

A1 Definitions and Interpretation

A1.1 Definitions

Unless the context otherwise requires the following terms shall have the meanings given to them below. Other capitalised terms shall have the meanings given to them in the Schedule in which they first appear.

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

"**Annex**" means an annex to a Schedule of this Contract.

"**Anti-Slavery Policy**" means the Authority's anti-slavery policy as set out in the relevant modern slavery statements and Government reports published from time to time.

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

"**Arbitration Notice**" means as it is described in clause I1.7 (Dispute Resolution).

"**Assignee**" means as it is described in clause F4.9 (Transfer and Sub-Contracting).

"**Associated Person**" has the meaning given to it in Section 44(4) of the Criminal Finances Act 2017.

"**Attachment of Earnings**" means an order made under Part 89 (Attachment of Earnings) of the Civil Procedure Rules instructing an employer to divert money from Defendant's wages/salary to pay back a debt or as otherwise may be defined by applicable Law from time to time.

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

"**Authority Contract Manager**" means the individual who shall have overall responsibility for the Authority's management of the Contract and "**Authority CM**" shall be construed accordingly.

"**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.

"**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 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 (Baseline Security Requirements) of Schedule 6 (Information Assurance and Security).

"**BCDR Plan**" means the Business Continuity and Disaster Recovery Plan as set out in Schedule 9 (Business Continuity and Disaster Recovery).

"**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.

"CCM" means the Commercial Contract Manager.

“CCN” means a change control notice in the form set out in Schedule 12 (Change Control).

“Certification Requirements” means the requirements in paragraph 6 (Certification Requirements) of Schedule 6 (Information Assurance and Security).

“CESG” means the Government’s Communications Electronics Security Group.

“Change” means a change in the Specification, the Price or 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.

"Change of Control" means as it is described in clause H1.3 (Insolvency and Change of Control).

"Change Request Form" means the change request form for completion by the Party requesting the Change as set out in Schedule 12 (Change Control).

"Charging Order" means an order made under Part 73 (Charging Orders, Stop Orders and Stop Notices) of the Civil Procedure Rules enabling the payment of a judgment debt to be secured by imposing a charge against certain types of the debtor’s capital assets or as otherwise may be defined by applicable Law from time to time.

"Code" means His Majesty's Government’s Supplier Code of Conduct.

“Commencement Date” means the date specified in clause A5.1 (Term).

"Commercial Contract Manager" means the person appointed by the Authority with responsibility for the overall commercial contract management of this Contract.

“Commercially Sensitive Information” means the information listed in Schedule 4 (Commercially Sensitive Information) 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.

“Complaint” means any communication received by the Supplier that expresses a negative comment regarding the Services provided and seeking specific redress.

“Comptroller and Auditor General” means the Government official responsible for supervising the quality of public accounting and financial reporting.

“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 and Special Categories of Personal Data within the meaning of the Data Protection Legislation. Confidential Information shall not include information which:

- (a) was public knowledge at the time of disclosure otherwise than by breach of clause E4 (Confidential Information);
- (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 documents the Parties expressly agree are included.

“Contracting Authority” means any contracting authority (other than the Authority) as defined in regulation 3 of the Regulations and **“Contracting Authorities”** shall be construed accordingly.

“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” has the meaning given in the UK GDPR.

“Copyright” has the meaning given in Part 1 of the Copyright, Designs and Patents Act 1988.

“Critical Service Level Failure” means a failure by the Supplier to provide the Services for a period of twenty-four (24) hours or more to meet the Target Performance Level.

“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.

"CRTPA" means the Contract (Rights of Third Parties) Act 1999.

"CSO" means Cyber Security Officer.

"Cyber Security Officer" means the person appointed by the Authority responsible for oversight of the Security Plan for this Contract.

"Data Loss Event" means any event that 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 Breach.

"Data Protection Impact Assessment" or "DPIA" means an assessment by the Controller carried out in accordance with section 3 of the UK GDPR and sections 64 and 65 of the DPA 2018.

"Data Protection Legislation" means:

- (a) all applicable UK Law relating to the processing of personal data and privacy, including but not limited to the UK GDPR, and the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy; and
- (b) (to the extent that it may be applicable) the EU GDPR.

"Data Protection Officer" has the meaning set out in the UK GDPR.

"Data Subject" has the meaning set out in the UK GDPR.

"Data Subject Access Request" or "DSAR" 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 the rights in databases as defined in section 3A, Chapter 1, Part 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. The term **"Defaulted"** shall be construed accordingly.

"Defendant" means the party accused of an offence in the Crown Court that has been means-tested and assessed to be liable or potentially liable for contributions towards their legal aid costs.

"Dispute Resolution Procedure" means the dispute resolution procedure set out at clause I1 (Dispute Resolution) of these Terms & Conditions.

"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 (Term).

“Enforcement Agent” means an enforcement agent, who is employed, appointed or certified by the courts to enforce writs or warrants, that is, to take control of a judgment debtor's goods and, if necessary, sell the goods in order to satisfy the debt.

“Enforcement Costs” means the costs associated with enforcing a case, and comprise Court Fees, Solicitors' Fees and Enforcement Fees, as further set out in paragraphs 2.9-2.14 of Schedule 2 (Pricing and Payment).

“Enhanced Monitoring” has the meaning in clause F.3 (Enhanced Monitoring).

“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.

“EU GDPR” has the meaning given in section 3 of the Data Protection Act 2018.

“Exit Day” has the meaning given to it in the European Union (withdrawal) Act 2018.

“Extension” means as defined in clause A5.2 (Term).

“Final Charging Order” means a court order confirming that a charge imposed by an Interim Charging Order remains in effect or as otherwise may be defined by applicable Law from time to time.

“Finance Officer” means the person appointed by the Authority with responsibility for overall financial management of this Contract.

“Financial Distress Event” means the occurrence of one or more of the events listed in paragraph 3.1 of Schedule 18 (Financial Distress).

“FO” means Finance Officer.

“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 either the Covid 19 pandemic or the United Kingdom's exit from the European Union and any related circumstances, events, changes or requirements.

"General Anti-Abuse Rule" means:

- (a) the legislation in Part 5 of the Finance Act 2013; and
- (b) 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.

[**"Guarantee"** means a deed of guarantee and indemnity for the benefit of the Authority in the form attached to this Contract at Schedule 17.]

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

"HMRC" means HM Revenue & Customs.

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

"Implementation Plan" means the agreed plan for implementation of the Services by the Supplier as further described in Schedule 15 (Implementation Plan).

"Indemnified Person(s)" means as it is defined in clause E7.3 (Intellectual Property Rights).

"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.

"Interim Charging Order" means an interim charging order made in accordance with rule 73.4(5), 73.4(6) or 73.6(3) of the Civil Procedure Rules or as otherwise may be defined in applicable Law from time to time.

"IP Materials" means as it is defined in clause E7.1 (Intellectual Property Rights).

"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 CESG or to an equivalent standard.

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

"Key Personnel" means the people named in Schedule 7 (Key Personnel) as key personnel.

"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).

"KPI" means the key performance indicators as set out in Schedule 8 (Performance, Management Information and Reporting).

"LAA" means the Legal Aid Agency.

"Law" means law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, right within the meaning of section 4(1) EU Withdrawal Act 2018 as amended by EU (Withdrawal Agreement) Act 2020, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any Regulatory Body with which the Supplier is bound to comply.

"Law Enforcement Processing" means processing under Part 3 of the DPA.

"LCIA" means the London Court of International Arbitration.

"Legal Aid Means Test Review", "MTR" or "Means Test Review" means the Government's review of the means test for legal aid as part of the Legal Support Action Plan.

"Logs" has the meaning given in clause E2.12 (Data Protection and Privacy).

"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.

"MAAT" means the Legal Aid Means Assessment Tool which is used by the Authority to record all case activity and decision making for a specific case and that provides a MAAT reference number/unique identifier for each case.

"Management Information" or "MI" means the management information that the Supplier shall provide the Authority in compliance with Schedule 8 (Performance, Management Information and Reporting).

“Material Breach” means a breach (including an anticipatory breach):

- (a) which has a material effect on the benefit which the Authority would otherwise derive from a substantial or material portion of the Contract; or
- (b) of any of the obligations set out in clauses D1 (Fraud and Bribery), E1 (Authority Data), E2 (Data Protection and Privacy), E3 (Official Secrets Acts and Finance Act), E4 (Confidential Information), E9 (Tax Compliance) or I4 (Conflicts of Interest); or
- (c) as otherwise identified as a "Material Breach" under the provisions of this Contract.

"Mediator" has the meaning set out in clause I1.5(a) (Dispute Resolution).

“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>.

“MSA” means the Modern Slavery Act 2015.

"MTR Change" means a Change resulting from the Legal Aid Means Test Review as further described in paragraph 11 of Schedule 1 (Specifications).

“NICs” means national insurance contributions.

"Notifiable Default" means:

- (a) the Supplier commits a Material Breach; and/or
- (b) the performance of the Supplier is likely to cause or causes a Critical Service Level Failure.

“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; and/or
 - 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.

"Open Book Data" means complete and accurate financial and non-financial information which is sufficient to enable the Authority to verify:

- (a) the Price already paid or payable and the Price forecast to be paid during the remainder of the Term;
- (b) the Supplier's costs and manpower resources broken down against each element of the Services;
- (c) the cost to the Supplier of engaging the Staff, including base salary, tax and pension contributions and other contractual employment benefits;
- (d) operational costs which are not included within the above, to the extent that such costs are necessary and properly incurred by the Supplier in the delivery of the Services;
- (e) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Services; and
- (f) the profit achieved over the Term and annually.

"Outcome" means either the decision of the court to acquit, convict or partially convict in a Crown Court trial case, or the successful/unsuccessful result of an appeal to Crown Court.

"Outgoing Supplier" means a supplier of services to the Authority before the Service Commencement Date that are the same as or substantially similar to the Services (or any part of the Services) and shall include any sub-contractor of such supplier (or any sub-contractor of any such sub-contractor).

"Performance Level" means the levels against which the performance of a KPI is measured, and as applicable, covers the target level to be achieved, and what constitutes a moderate failure level and a critical failure level.

"Personal Data" has the meaning set out in the UK GDPR.

"Personal Data Breach" has the meaning set out in the UK GDPR.

"Policies and Standards" means the policies and standards as set out in Schedule 14 (Policies and Standards).

"Premises" means the location where the Services are supplied.

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

"Processor" has the meaning set out in the UK GDPR.

"Prohibited Act" means:

- i) to directly or indirectly offer, promise or give any person working for or engaged by the Authority a financial or other advantage to: 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 limb (c) above if such activity, practice or conduct has been carried out in the UK.

“Property” means that property, other than real property, issued or made available to the Supplier by the Authority in connection with the Contract.

“Protective Measures” means appropriate technical and organisational measures designed to ensure compliance with obligations of the Parties arising under Data Protection Legislation and this Contract, 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.

“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 Standardisation or other reputable or equivalent body (and their successor bodies) with which 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.

“Receipt” means the physical or electronic arrival of an invoice at the address specified in paragraph 9.4 of Schedule 2 or at any other address given by the Authority to the Supplier for the submission of invoices from time to time.

“Rectification Plan” means a plan produced by the Supplier in accordance with clause F2 (Rectification Plan Process) designed to rectify a Service Level Failure.

“Regulations” means the Public Contract Regulations 2015 (SI 2015/102).

“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 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 substantially similar to any of the Services in substitution for any 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.

“Review” means as it is described in clause F1.2 (Contract Performance).

“Review Report” has the meaning set out in clause F1.4 (Contract Performance).

“SBO” means Senior Business Owner.

“Senior Business Owner” means the person appointed by the Authority with responsibility for the overall operational management of this Contract.

“Schedule” means a schedule to this Contract.

“Security Plan” means the plan prepared by the Supplier which includes the matters set out in paragraph 3.2 (Security Plan) of Schedule 6 (Information Assurance and Security).

“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.

“Service Commencement Date” means the date on which the provision of the Services commence in accordance with clause A5.1 of these Terms & Conditions.

“Service Costs” means the total value of the Unit of Work Prices completed in the relevant monthly invoice period.

"Service Credits" means payments that are to be made to the Supplier to reward it for performance that exceeds the Target Performance Levels for KPIs 1-3 in Schedule 8 (Performance, Management and Reporting).

"Service Debits" means deductions to the Price that are made where the Supplier's performance is below the Target Performance Levels set out in Schedule 8 (Performance, Management and Reporting).

"Service Level Failure" means a failure by the Supplier to provide the Services to meet the Target Performance Level.

"Services" means the services set out in Schedule 1 (Specifications) (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>

"Special Categories of Personal Data" has the meaning given in the UK GDPR.

"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 (Specification) including, where appropriate, the Key Personnel, the Premises and 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.

"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 Services under this 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 Contract Manager" means the individual who shall have the overall responsibility for the Supplier's management of the Contract and **"Supplier CM"** shall be construed accordingly.

"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 and Third Party Software).

"Supplier System" means the information and communications technology system used by the Supplier in performing the Services including the Supplier 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
- (c) such earlier date of termination or partial termination of the Contract in accordance with the Law or the Contract.

“Terms & Conditions” means these terms and conditions.

“Third Party Beneficiary” means as it is defined in clause I5.1 (Rights of Third Parties).

“Third Party IP Claim” has the meaning given to it in clause E7.5 (Intellectual Property Rights).

“Third Party Provision(s)” means as it is defined in clause I5.1 (Rights of Third Parties).

“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 and which is specified as such in Schedule 5 (Supplier and Third Party Software).

“Transferee” means as it is described in clause F4.15 (Transfer and Sub-Contracting).

“Transferring Employee” means those employees of an Outgoing Supplier to whom TUPE applies on the Service Commencement Date.

“TUPE” means the Transfer of Undertakings (Protection of Employment) Regulations 2006.

“TUPE Information” means the information set out in clause B10.1 (Employment).

“UK GDPR” means the UK General Data Protection Regulation, and has the meaning given in section 3 of the Data Protection Act 2018.

“Valid Invoice” means an invoice containing the information set out in clause C1.5 (Payment and VAT).

“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.

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

A1.2 Interpretation

In the Contract, unless the context implies otherwise:

- (a) the singular includes the plural and vice versa;
- (b) reference to any gender includes any other;
- (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; and
- (j) any reference in the Contract which immediately before Exit Day was a reference to (as it has effect from time to time):
 - i) any EU regulation, EU decision, EU tertiary legislation or provision of the European Economic Area (“EEA”) agreement (“EU References”) which is to form part of domestic law by application of section 3 of the European Union (Withdrawal) Act 2018 shall be read as a reference to the EU References as they form part of domestic law by virtue of section 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 as a reference to the UK institution, authority or body to which its functions were transferred;
- (k) if there is any conflict between the clauses and the Schedules and/or any Annexes to the Schedules, the conflict shall be resolved in accordance with the following order of precedence:

- i) the clauses and definitions;
- ii) the Schedules and their Annexes;

and in the event that the conflict cannot be resolved in accordance with the order of precedence set out in this clause A1.2(k), then decision of the Authority upon the matter shall be final and conclusive.

A2 Authority Obligations

- A2.1 Save as 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 on, 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 [Redacted] (the "**Commencement Date**") and ends on 2nd February 2029 (the "**End Date**") unless it is terminated early or extended in accordance with the Contract. The Services starts on 3rd February 2025 (the "**Service Commencement Date**").
- A5.2 The Authority may, at its sole discretion and subject to clause A5.3 below, extend the Term of the Contract on any number of occasions and for any period provided that the aggregate duration of all Extensions may not exceed twenty-four (24) months ("**Extension**"). The terms of the Contract will apply throughout the period of any Extension.
- A5.3 To extend the Term of the Contract, pursuant to clause A5.2 above, the Authority will give the Supplier notice of one (1) month before the expiry of the current End Date and any subsequent Extension.

A6 Contract Management

- A6.1 The Supplier shall comply with the contract management requirements as set out in Schedule 13 (Governance and Contract Management).

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 (Payment and VAT).
- B1.2 The terms and conditions contained 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.
- B1.3 On or before the Service Commencement Date if required by the Authority the Supplier shall procure the execution and delivery to the Authority of the Guarantee.

B2 Delivery of the Services

- B2.1 The Supplier shall provide the Services from the Service Commencement Date. 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 those Staff are properly managed and supervised; and
 - (c) comply with the standards and requirements set out in clause D (Statutory Obligations and Corporate Social Responsibility) and Schedule 14 (Policies and Standards).
- B2.4 If the Specification includes installation of equipment the Supplier shall notify the Authority in writing when it has completed installation. Following receipt of such notice, the Authority shall inspect the installation and shall, by giving notice to the Supplier: accept the installation; or

- (a) reject the installation and inform the Supplier why, in the Authority's reasonable opinion, the installation does not satisfy the Specification.
- B2.5 If the Authority rejects the installation pursuant to clause B2.4(b) above, the Supplier shall immediately rectify or remedy any defects and if, in the Authority's reasonable opinion, the installation does not, within two (2) Working Days or such other period agreed by the Parties, comply with the Specification, the Authority may terminate the Contract with immediate effect.
- B2.6 The installation is complete when the Supplier receives a notice issued by the Authority in accordance with clause B2.4(a) above. Notwithstanding acceptance of any installation in accordance with clause B2.4(a), the Supplier is solely responsible for ensuring that the Services and the installation conform to the Specification. No rights of estoppel or waiver shall arise as a result of the acceptance by the Authority of the installation.
- B2.7 During the Term, the Supplier shall:
 - (a) at all times have all licences, Approvals and consents necessary to enable the Supplier and Staff to carry out the installation;
 - (b) provide all tools and equipment (or procure the provision of all tools and equipment) necessary for completion of the installation; and
 - (c) not, in delivering the Services, in any manner endanger the safety or convenience of the public.
- B2.8 The Authority may inspect the manner in which the Supplier supplies the Services at the Premises during normal business hours on reasonable notice. The Supplier shall provide at its own cost all such facilities as the Authority may reasonably require for such inspection. In this clause B2, Services include planning or preliminary work in connection with the supply of the Services.
- 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 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.

B3 Equipment

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

- B3.2 The Supplier shall not deliver any Equipment to, or begin any work on, the Premises without Approval.
- 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 If the Authority reimburses the cost of any Equipment to the Supplier the Equipment shall become the property of the Authority and shall on request be delivered to the Authority as directed by the Authority. The Supplier shall keep a full and accurate inventory of such Equipment and deliver that inventory to the Authority on request and on completion of the Services.
- B3.6 The Supplier shall maintain all Equipment in a safe, serviceable and clean condition.
- B3.7 The Supplier shall, at the Authority's written request, at its own cost and as soon as reasonably practicable:
- (a) remove immediately from the Premises Equipment which is, in the Authority's opinion, hazardous, noxious or not supplied in accordance with the Contract; and
 - (b) replace such item with a suitable substitute item of Equipment.
- B3.8 Within twenty (20) Working Days of the end of the Term, the Supplier shall remove the Equipment together with any other materials used by the Supplier to supply the Services and shall leave the Premises in a clean, safe and tidy condition. The Supplier shall make good any damage to those Premises and any fixtures and fitting in the Premises which is caused by the Supplier or Staff.

B4 Key Personnel

- B4.1 The Supplier acknowledges that Key Personnel are essential to the proper provision of the Services and shall ensure that the Key Personnel fulfil their roles at all times during the Contract Term. Schedule 7 (Key Personnel) sets out the Supplier's Key Personnel.
- B4.2 Key Personnel shall not be released from supplying the Services without Approval except by reason of long-term sickness, maternity leave, paternity leave or termination of employment or other similar extenuating circumstances.
- B4.3 The Authority may interview and assess any proposed replacement for Key Personnel and any replacements to Key Personnel are subject to Approval. Such replacements shall be of at least equal status, experience and skills to Key Personnel being replaced and be suitable for the responsibilities of that person in relation to the Services.
- B4.4 The Authority shall not unreasonably withhold Approval under clauses B4.2 or B4.3 and such Approval is conditional on appropriate arrangements being made by the Supplier to minimise any adverse effect on the Services which could be caused by a change in Key Personnel.

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 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 Supplier shall not, and shall procure that all Staff shall not, take photographs on the Authority's Premises without Approval.

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

B6 Due Diligence

Save as the Authority may otherwise direct, the Supplier is deemed to have inspected the Premises before submitting its Tender and to have completed due diligence in relation to all matters connected with the performance of its obligations under the Contract.

B7 Licence to Occupy

B7.1 Any land or Premises made available from time to time to the Supplier by the Authority

in connection with the Contract are on a non-exclusive licence basis free of charge and are used by the Supplier solely for the purpose of performing its obligations under the Contract. The Supplier has the use of such land or Premises as licensee and shall vacate the same on termination of the Contract.

- B7.2 The Supplier shall limit access to the land or Premises to such Staff as is necessary for it to perform its obligations under the Contract and the Supplier shall co-operate (and ensure that its Staff co-operate) with other persons working concurrently on such land or Premises as the Authority may reasonably request.
- B7.3 If the Supplier requires modifications to the Authority's Premises such modifications are subject to Approval and shall be carried out by the Authority at the Supplier's cost.
- B7.4 The Supplier shall (and shall ensure that any Staff on the Authority's Premises shall) observe and comply with such rules, regulations and requirements (including those relating to security arrangements) as may be in force from time to time for the conduct of personnel when on the Authority's Premises as determined by the Authority.
- B7.5 The Contract does not create a tenancy of any nature in favour of the Supplier or its Staff and no such tenancy has or shall come into being and, notwithstanding any rights granted pursuant to the Contract, the Authority may use the Premises owned or occupied by it in any manner it sees fit.

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 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 five (5) Working Days of receipt.
- B8.3 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.
- B8.4 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.
- B8.5 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.
- B8.6 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.

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 six (6) months thereafter.
- B9.2 If either Party breaches clause B9.1 above, it shall pay the other Party a sum equivalent to [Redacted] payable by the Party in breach in respect of the first year of a 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.

B10 Employment

- B10.1 Subject to clause B10.2, the Authority indemnifies and keeps indemnified the Supplier against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and other liabilities which the Supplier may suffer or incur as a result of or in connection with:
- (a) any claim or demand by any Transferring Employee (whether in contract, tort, under statute, pursuant to EU Law or otherwise) in each case arising directly or indirectly from any act, fault or omission of the Outgoing Supplier or any of their Sub-Contractors in respect of any Transferring Employee on or before the start of this Contract; and
 - (b) any failure by the Outgoing Supplier or any of its Sub-Contractors to comply with its obligations under regulations 13 or 14 of TUPE or any award of compensation under regulation 15 of TUPE save where such failure arises from the failure of the Supplier or any Sub-Contractor to comply with its duties under regulation 13 of TUPE.
- B10.2 The indemnity from the Authority at B10.1 will only apply to the extent that the Authority recovers any sum in respect of the subject matter of the indemnity from such Outgoing Supplier under any indemnity or other legal entitlement it has against such Outgoing Supplier. The Authority will use all reasonable endeavours to recover any such sums under any such entitlement.
- B10.3 No later than twelve (12) months prior to the end of the Term, the Supplier shall fully and accurately disclose to the Authority all information the Authority may reasonably request in relation to the Staff including the following:
- (c) the total number of Staff whose employment/engagement terminates at the end of the Term, save for any operation of Law;
 - (d) the age, gender, salary or other remuneration, future pay settlements and

- redundancy and pensions entitlement of the Staff referred to in clause B10.1(a);
 - (e) the terms and conditions of employment/engagement of the Staff referred to in clause B10.1(a), their job titles and qualifications;
 - (f) their immigration status;
 - (g) details of any current disciplinary or grievance proceedings ongoing or circumstances likely to give rise to such proceedings and details of any claims current or threatened; and
 - (h) details of all collective agreements with a brief summary of the current state of negotiations with any such bodies and with details of any current industrial disputes and claims for recognition by any trade union.
- B10.4 At intervals determined by the Authority (which shall not be more frequent than once per calendar month) the Supplier shall give the Authority updated TUPE Information.
- B10.5 Each time the Supplier supplies TUPE Information to the Authority it warrants its completeness and accuracy and the Authority may assign the benefit of this warranty to any Replacement Supplier.
- B10.6 The Authority may use TUPE Information it receives from the Supplier for the purposes of TUPE and/or any retendering process in order to ensure an effective handover of all work in progress at the end of the Term. The Supplier shall provide the Replacement Supplier with such assistance as it shall reasonably request.
- B10.7 If TUPE applies to the transfer of the Services on termination of the Contract, the Supplier indemnifies and keeps indemnified the Authority, the Crown and any Replacement Supplier against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and other liabilities which the Authority or the Crown or any Replacement Supplier may suffer or incur as a result of or in connection with:
- (a) the provision of TUPE Information;
 - (b) any claim or demand by any Returning Employee (whether in contract, tort, under statute, pursuant to EU Law or otherwise) in each case arising directly or indirectly from any act, fault or omission of the Supplier or any Sub-Contractor in respect of any Returning Employee on or before the end of the Term;
 - (c) any failure by the Supplier or any Sub-Contractor to comply with its obligations under regulations 13 or 14 of TUPE or any award of compensation under regulation 15 of TUPE save where such failure arises from the failure of the Authority or a Replacement Supplier to comply with its duties under regulation 13 of TUPE;
 - (d) any claim (including any individual employee entitlement under or consequent on such a claim) by any trade union or other body or person representing any Returning Employees arising from or connected with any failure by the Supplier or any Sub-Contractor to comply with any legal obligation to such trade union, body or person; and

- (e) any claim by any person who is transferred by the Supplier to the Authority and/or a Replacement Supplier whose name is not included in the list of Returning Employees.

B10.8 If the Supplier is aware that TUPE Information has become inaccurate or misleading, it shall notify the Authority and provide the Authority with up to date and accurate TUPE Information.

B10.9 This clause B10 applies during the Term and indefinitely thereafter.

B10.10 The Supplier undertakes to the Authority that, during the twelve (12) months prior to the end of the Term the Supplier shall not (and shall procure that any Sub-Contractor shall not) without Approval (such Approval not to be unreasonably withheld or delayed):

- (a) amend or vary (or purport to amend or vary) the terms and conditions of employment or engagement (including, for the avoidance of doubt, pay) of any Staff (other than where such amendment or variation has previously been agreed between the Supplier and the Staff in the normal course of business and where any such amendment or variation is not in any way related to the transfer of the Services);
- (b) terminate or give notice to terminate the employment or engagement of any Staff (other than in circumstances in which the termination is for reasons of misconduct or lack of capability);
- (c) transfer away, remove, reduce or vary the involvement of any other Staff from or in the provision of the Services other than where such transfer or removal: (i) was planned as part of the individual's career development; (ii) takes place in the normal course of business; and (iii) will not have any adverse impact upon the delivery of the Services by the Supplier, (provided that any such transfer, removal, reduction or variation is not in any way related to the transfer of the Services); or
- (d) recruit or bring in any new or additional individuals to provide the Services who were not already involved in providing the Services prior to the relevant period.

B11 Welsh Language Requirements

B11.1 The Supplier shall, at all times, comply with the Welsh Language Act 1993 and the Authority's Welsh Language Scheme (as amended from time to time) as if it were the Authority to the extent that the same relate to the provision of the Services.

B11.2 The Supplier shall be responsible for promoting the delivery of the Services in Welsh or English to the recipients of the Services and shall use reasonable endeavours to achieve this.

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 (Pricing and Payment).
- C1.2 The Authority shall, 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.
- C1.3 The Supplier shall 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.
- C1.4 All the Supplier's invoices shall be expressed in sterling or any other currency which is Approved.
- C1.5 A Valid Invoice is an invoice which includes:
- (a) the Supplier's full name, address and title of the Contract;
 - (b) the invoice reference number and corresponding remittance reference number;
 - (c) the Purchase Order number;
 - (d) the Supplier's VAT number;
 - (e) the date of the invoice and the dates of the period covered by the invoice;
 - (f) the Supplier's sort code and account number;
 - (g) an accurate breakdown of Service Costs, Enforcement Costs and/or Service Credits of Service Debits, by case type;
 - (h) case level detail, ordered by Supplier ID reference number and Authority MAAT reference numbers; and
 - (i) if requested by the Authority:
 - i) timesheets for Staff engaged in providing the Services signed and dated by the Authority's representative on the Premises on the day;
 - ii) the name of the individuals to whom the timesheet relates and hourly rates for each;
 - iii) identification of which individuals are the Supplier's Staff and which are any Sub-Contractors' staff;
 - iv) the address of the Premises and the date on which work was undertaken;
 - v) the time spent working on the Premises by the individuals concerned;

vi) details of the type of work undertaken by the individuals concerned;

vii) details of plant or materials operated and on standby;

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

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

- 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 Not used.
- C1.8 Not used.
- C1.9 Not used.
- 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 Authority shall pay all sums due to the Supplier within thirty (30) calendar days of Receipt of a Valid Invoice, unless an alternative arrangement has been Approved. Valid Invoices should be submitted for payment to the following email address:
- [Redacted]** <mailto:CCMT@laa.cjsm.net>
- C1.14 If the Authority fails to pay any undisputed Valid Invoices under this Contract, the Supplier shall have the right to charge interest on the overdue amount at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgment.
- C1.15 The Supplier shall ensure that a provision is included in all Sub-Contracts which requires payment to be made of all sums due to Sub-Contractors within thirty (30) calendar days from the Receipt of a Valid Invoice.
- C1.16 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 C1.16 shall be paid by the Supplier to the Authority not less than five (5) Working Days before the date upon which the tax or other liability is

payable by the Authority.

C1.17 The Supplier shall not suspend the Services unless the Supplier is entitled to terminate the Contract under clause H2.3 (Termination on Default) for failure to pay undisputed sums of money.

C1.18 The Authority may reject an invoice which is not a Valid Invoice.

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 (Pricing and Payment) and clause F6 (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. STATUTORY OBLIGATIONS AND CORPORATE SOCIAL RESPONSIBILITY

D1 His Majesty's Government's Supplier Code of Conduct

D1.1 The Code sets out the standards and behaviours expected of suppliers who work with Government. The Code can be found online at:

[Supplier Code of Conduct - v2 \(publishing.service.gov.uk\)](https://publishing.service.gov.uk)

D1.2 The Supplier shall, and shall procure that its Sub-Contractors shall:

- (a) comply with its legal obligations, in particular those in clauses D2 (Fraud and Bribery), D3 (Equality and Accessibility), D4 (Health and Safety), D5 (Modern Slavery Act), D6 (Income Security), D7 (Working Hours), D8 (Right to Work), and meet the standards set out in the Code as a minimum; and
- (b) use reasonable endeavours to comply with the standards in D9 (Corporate Social Responsibility).

D2 Fraud and Bribery

D2.1 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.

D2.2 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.

D2.3 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 clause D2.3(a) and D2.3(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.

D2.4 The Supplier shall immediately notify the Authority in writing if it becomes aware of any breach of clauses D2.1 and/or D2.2, 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.
- D2.5 If the Supplier notifies the Authority pursuant to clause D2.4, 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.
- D2.6 If the Supplier is in Default under clauses D2.1 and/or D2.2, 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.
- D2.7 Any notice served by the Authority under clause D2.6 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).

D3 Equality and Accessibility

- D3.1 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), including the Equality Act 2010 and Breathing Space Regulations 2020;
 - 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).
- D3.2 The Supplier will make reasonable adjustments for individuals with disabilities in its

provision of the Services. The Supplier may not pass any costs of such adjustments on to the Defendant.

D3.3 Reasonable adjustments for individuals with disabilities may include, but are not limited to, the following:

- (a) alternative formats for written correspondence. This could include, in rare cases, braille or audio, and more frequently large print; and
- (b) further assistance, should an individual not understand correspondence or information received from the Supplier.

D3.4 Where reasonable adjustments have been made, the Supplier will record the Defendant's preferred or required format of communication on their internal systems.

D3.5 The Supplier must operate an equal opportunities policy in relation to recruitment of Staff.

D3.6 The Supplier will ensure that all documents and correspondence it produces in the course of delivering the Service shall meet plain language standards.

D3.7 The Supplier must ensure that it pursues debts in a timely manner and that the timetable for the recovery of debts is complied with. The Supplier must also recognise that some debtors are vulnerable and will require a more sympathetic, sensitive, and practical approach to debt recovery. The Authority and the Supplier will take account of the needs of all defendants throughout the debt recovery process.

D3.8 The Supplier must adhere to the National Standards for Enforcement Agents and the FCA Principles of Business and Consumer Credit Rulebook as set out in Schedule 14 (Policies and Standards) in relation to vulnerable clients.

D3.9 The Supplier will use a standardised financial statement form/method as agreed with the Authority to calculate income and outgoings when determining affordable payment plans and will make use of signposting to debt advice charities when dealing with vulnerable debtors or those who have expressed difficulties in paying any debts.

D4 Health and Safety

D4.1 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 (as set out in Schedule 14 (Policies and Standards)) while at the Authority's Premises.

D4.2 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 associated safety measures in order to manage the risk.

D5 Modern Slavery Act

- D5.1 The Supplier shall, and procure that each of its Sub-Contractors shall, comply with:
- (a) the MSA; and
 - (b) the Anti-Slavery Policy.
- D5.2 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 in connection with 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.
- D5.3 The Supplier represents, warrants and undertakes during 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; and
 - (b) 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 subject to any investigation, inquiry or enforcement proceedings by any governmental, administrative or regulatory body regarding any offence in connection with slavery and trafficking.
- D5.4 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 is connected with the Contract.
- D5.5 If the Supplier notifies the Authority pursuant to clause D5.4, 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.

D5.6 If the Supplier is in Default under clauses D5.2 or D5.3 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.

D6 Income Security

D6.1 The Supplier shall:

- (a) ensure that all pay and benefits paid to the Staff 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 Staff 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; and
- (d) record all disciplinary measures taken against Staff.

D7 Working Hours

D7.1 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 forty-eight (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 (7) day period shall not exceed sixty (60) hours, except where covered by paragraph D7.1(e);
- (e) working hours do not exceed sixty (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 Staff are provided with at least:
 - i) one (1) day off in every seven (7) day period; or
 - ii) where allowed by Law, two (2) calendar days off in every fourteen (14) day period.

D8 Right to Work

D8.1 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.

D9 Corporate Social Responsibility

D9.1 Zero Hours Contracts

D9.1.1 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.

D9.1.2 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.

D9.2 Sustainability

D9.2.1 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 Services;
- (c) maintain ISO 14001 or BS 8555 or an equivalent standard intended to manage its environmental responsibilities; and
- (d) 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.

E PROTECTION OF INFORMATION

E1 Authority Data

E1.1 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 immediately upon 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 (Information Assurance and Security).
- E1.2 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.

E2 Data Protection and Privacy

- E2.1 The Parties acknowledge that for the purposes of Data Protection Legislation, the Authority is the Controller, and the Supplier is the Processor. The only processing which the Authority has authorised the Supplier to do is listed in Schedule 10 (Data Processing) and may not be determined by the Supplier. The term "**processing**" and any associated terms are to be read in accordance with Article 4 of the UK GDPR.
- E2.2 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 this Contract:
- i) process that Personal Data only in accordance with Schedule 10 (Data Processing) 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, which the Authority may reasonably reject. In the event of the Authority reasonably rejecting Protective Measures put in place by the Supplier, the Supplier must propose alternative Protective Measures to the satisfaction of the Controller. Failure to reject shall not amount to Approval by the Authority of the adequacy of the Protective Measures. Protective Measures must take account of the:
 - A) nature of the data to be protected;
 - B) harm that might result from a Data Loss Event;
 - C) state of technological development; and
 - D) 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 10);
 - 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 E2;
 - 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 otherwise allowed under 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 UK unless Approved and:

- i) the destination country has been recognised as adequate by the UK Government in accordance with Article 45 of the UK GDPR or section 74 of the DPA;
 - ii) the Authority or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 of the DPA) as determined by the Authority;
 - iii) the Data Subject has enforceable rights and effective legal remedies;
 - iv) 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
 - v) 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 E2.3, notify the Authority immediately if it:
 - i) receives a Data Subject Access Request (or purported Data Subject Access 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.

E2.3 The Supplier's obligation to notify under clause E2.2(g) includes the provision of further information to the Authority, as details become available.

E2.4 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 E2.2(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 Access 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.

E2.5 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with clause E2. 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 UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
- (c) is likely to result in a risk to the rights and freedoms of Data Subjects.

E2.6 The Supplier shall allow audits of its Data processing activity by the Authority or the Authority's designated auditor.

E2.7 Each Party shall designate a Data Protection Officer if required by the Data Protection Legislation.

E2.8 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 clause E2 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.

E2.9 The Supplier remains fully liable for the acts and omissions of any Sub-Processor.

E2.10 The Parties shall take account of any guidance published by the Information Commissioner's Office and, notwithstanding the provisions of clause F5 (Change), the

Authority may on not less than thirty (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.

E2.11 In relation to Law Enforcement Processing of Personal Data, 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.

E2.13 This clause E2 applies during the Term and indefinitely after its expiry.

E3 Official Secrets Acts and Finance Act

E3.1 The Supplier shall comply with:

- (a) the Official Secrets Acts 1911 to 1989; and
- (b) section 182 of the Finance Act 1989.

E4 Confidential Information

E4.1 Except to the extent set out in this clause E4 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.

E4.2 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 but with any information which is exempt from disclosure, in accordance with the provisions of the FOIA, redacted. The Authority shall, prior to publication, consult with the Supplier on the manner and format of publication and to inform its decision regarding any redactions but shall have the final decision in its absolute discretion.

E4.3 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 E4.3.

E4.4 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.

E4.5 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.

E4.6 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.

E4.7 Clause E4.1 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.

E4.8 Nothing in clause E4.1 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 E4.8(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.

E4.9 Nothing in clauses E4.1 to E4.6 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.

E4.10 The Authority shall use reasonable endeavors 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 E4.8 is made aware of the Authority's obligations of confidentiality.

- E4.11 If the Supplier does not comply with clauses E4.1 to E4.8 the Authority may terminate the Contract immediately on notice.
- E4.12 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.
- E4.13 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 E4.12.

E5 Freedom of Information

- E5.1 The Supplier acknowledges that the Authority is subject to the requirements of the FOIA and the EIR.
- E5.2 The Supplier shall transfer to the Authority all Requests for Information that it receives as soon as practicable and in any event within two (2) Working Days of receipt and shall:
- (a) give the Authority a copy of all Information in its possession or control in the form that the Authority requires within five (5) Working Days (or such other period as the Authority may specify) of the Authority's request;
 - (b) 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
 - (c) not respond directly to a Request for Information unless authorised to do so in writing by the Authority.
- E5.3 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.

E6 Publicity, Media and Official Enquiries

E6.1 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 announcements 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.

E6.2 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.

E6.3 The Supplier shall use reasonable endeavours to ensure that its Staff, professional advisors and consultants comply with clause E6.1.

E7 Intellectual Property Rights

E7.1 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 His Majesty the King) 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.

E7.2 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 His Majesty the King, 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.

E7.3 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 Person(s)**");
- (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 E7.3, 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.

E7.4 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.

E7.5 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).

E7.6 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 E7.6 in relation to any costs and expenses to the extent that such arise directly from the matters referred to in clauses E7.3(d)i) and ii).

E7.7 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.

E7.8 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 E7.3(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;
- (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; or

if the Supplier is unable to comply with clauses E7.8(a) or (b) within twenty (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.

E7.9 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).

E8 Audit

E8.1 The Supplier shall:

- (a) keep and maintain until six (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 its compliance with, and discharge of its obligations under 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; and

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

E8.2 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 eighteen (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 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.

E8.3 The Supplier (and its agents) shall permit 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 conducting a 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.

- E8.4 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 fifteen (15) Working Days' notice of its intention to conduct an audit.
- E8.5 The Parties bear their own respective costs and expenses incurred in respect of compliance with their obligations under clause E8, 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.

E9 Tax Compliance

- E9.1 If, during the Term, an Occasion of Tax Non-Compliance occurs, the Supplier shall:
- (a) notify the Authority in writing of such fact within five (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.
- E9.2 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.

F. CONTROL OF THE CONTRACT

F1 Performance Review

- F1.1 Without prejudice to the Supplier's obligations under clause B2.1 and Schedule 8 (Performance, Management and Reporting), 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 proposed corrective action and the date by which that action will be completed.

- F1.2 If or when, for whatever reason, the Supplier's CM identifies any potential problems in meeting the requirements of the Contract, these should be brought to the Authority CM's attention within two (2) Working Days except where specified otherwise.
- F1.3 At or around six (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.
- F1.4 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.
- F1.5 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.
- F1.6 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.
- F1.7 The Supplier shall, within ten (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.
- F1.8 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 Rectification Plan Process

- F2.1 Within five (5) Working Days of receipt of the Authority's notice pursuant to paragraph 4 (Service Level Failure) of Schedule 8 (Performance, Management and Reporting) and

clause H2 (Termination on Default) the Supplier shall submit a draft Rectification Plan to the Authority for review, along with any further documentation that the Authority reasonably requires in order to assess the draft Rectification Plan. The draft Rectification Plan must set out:

- a) full details of the Critical Service Level Failure and/or Service Level Failure that has occurred, including a root cause analysis;
- b) the actual or anticipated effect of the Critical Service Level Failure and/or Service Level Failure; and
- c) steps which the Supplier proposes to take to rectify the Critical Service Level Failure and/or Service Level Failure (if applicable) and to prevent such Critical Service Level Failure and/or Service Level Failure from recurring, including timescales for such steps and for the rectification of the Critical Service Level Failure and/or Service Level Failure (where applicable).

F2.2 The Authority shall, acting reasonably, accept or reject the draft Rectification Plan and shall notify the Supplier of its decision as soon as reasonably practicable. If the Authority rejects the draft Rectification Plan, the Authority shall give reasons for its decision and the Supplier shall take the reasons into account in the preparation of a revised Rectification Plan. The Supplier shall submit the revised draft of the Rectification Plan to the Authority for review within five (5) Working Days (or such other period as agreed between the Parties) of the Authority's notice rejecting the first draft (and this process may be repeated as many times as the Authority requires). If the Authority consents to the Rectification Plan, the Supplier shall immediately start work on the actions set out in the Rectification Plan.

F2.3 If the Supplier fails to fully implement the Rectification Plan in accordance with its terms, the Authority may:

- a) make such arrangements through another provider, third party or by itself, to provide and perform the Services in whole or in part to which the Supplier is in Default. Any expenditure incurred performing the Services Defaulted by the Supplier shall be paid in full by the Supplier to the Authority upon request; and
- b) treat such failure as a Material Breach and terminate the Contract pursuant to clause H2.1(c).

F2.4 For as long as the Rectification Plan is in place and/or a Critical Service Level Failure has occurred then:

- a) the Service Credits and Service Debits that would otherwise have accrued during the relevant Service period shall not accrue; and
- b) the Authority shall be entitled to withhold and retain as compensation a sum equal to any charges which would otherwise have been due to the Supplier in respect of that Service period.

F2.5 The operation of clause F2.4 shall be without prejudice to the right of the Authority to terminate this Contract and/or to claim damages from the Supplier for Material Breach.

F2.6 If the Supplier fails to:

- a) submit a Rectification Plan or a revised Rectification Plan within the timescales set out in clauses F2.1 or F2.2; and
- b) adhere to the timescales set out in an accepted Rectification Plan to resolve the Notifiable Default.

or if the Authority otherwise rejects a Rectification Plan, the Authority can require the Supplier to attend an Escalation Meeting on not less than five (5) Working Days' notice. The Authority will determine the location, time and duration of the Escalation Meeting(s) and the Supplier must ensure that the Supplier CM is available to attend.

F2.7 The Escalation Meeting(s) will continue until the Authority is satisfied that the Notifiable Default has been resolved, however, where an Escalation Meeting(s) has continued for more than five (5) Working Days, either Party may treat the matter as a dispute to be handled through the Dispute Resolution Procedure.

F2.8 If the Supplier is in Default of any of its obligations under this clause F2, the Authority shall be entitled to terminate this Contract and the consequences of termination set out in clause H5 shall apply as if the Contract were terminated under clause H2.

F.3 Enhanced Monitoring

F.3.1 On the occurrence of any Enhanced Monitoring trigger as further provided in paragraph 4.1 of Schedule 8 (Performance, Management Information and Reporting), the Authority may by written notice to the Supplier increase the level of its monitoring of the Supplier's performance or require the Supplier to increase the level of its monitoring and reporting of its own performance of its obligations under the Contract in respect of the Services (or relevant part thereof) to which Enhanced Monitoring applies, until such time as the circumstances giving rise to Enhanced Monitoring no longer apply, but in any event for not more than a period of six (6) months after the giving of such notice, unless the Supplier has failed to satisfy the requirements of clause F3.2 during that six month period, in which case the Authority may, at its sole discretion and without prejudice to its other rights, elect to extend the period of Enhanced Monitoring by, at most a further six (6) months.

F3.2 Enhanced Monitoring that the Authority may require under clause F3.1 may include:

- (a) increasing the frequency, depth or types of any existing monitoring or reporting;
- (b) adding new reporting and/or monitoring requirements
- (c) requiring the Supplier to provide a reasonable number of appropriately qualified and senior staff to participate in an existing or dedicated governance board or other focus group established by the Authority; and/or
- (d) the provision of Open Book Data,

in relation to the obligations which give rise to the Enhanced Monitoring.

- F3.3 Any such notice to the Supplier (as referred to in clause F3.1) shall specify in reasonable detail the additional measures to be taken by the Authority or by the Supplier (as the case may be) in monitoring or reporting on the performance of the Supplier.
- F3.4 The Supplier shall notify the Authority within five (5) Working Days of receipt of the notice referred to in clause F3.1 of any measures specified in such notice that the Supplier (acting reasonably) believes are excessive or may prejudice the Suppliers performance of its obligations under the Contract, together with such alternative measures that the Supplier may propose.
- F3.5 The Supplier shall bear its own costs and shall reimburse the Authority in respect of any additional costs that are directly incurred by the Authority in the taking of any action under this clause F3.

F4 Remedies

- F4.1 Without prejudice to any rights that the Authority may have under Schedule 8, 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; and/or
 - (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; and/or
 - (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.
- F4.2 Without prejudice to its right under clause C2 (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.
- F4.3 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.

- F4.4 If the Supplier has been notified of a failure in accordance with clause F3.3 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.
- F4.5 If the Supplier has been notified of a failure in accordance with clause F3.3, 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 F3.5 and the progress of those measures until resolved to the satisfaction of the Authority.
- F4.6 If, having been notified of any failure, the Supplier does not remedy it in accordance with clause F3.5 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.

F5 Transfer and Sub-Contracting

- F5.1 Except where both clauses F5.9 and F5.10 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.
- F5.2 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.
- F5.3 The Supplier shall ensure that Sub-Contractors retain all records relating to the Services for at least six (6) years from the date of their creation and make them available to the Authority on request in accordance with clause E8 (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.
- F5.4 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 Sub-Contract 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 E1 (Authority Data) and E2 (Data Protection and Privacy);
- (b) the Sub-Contractor includes a provision having the same effect as set out in clause F54(a) in any Sub-Contract which it awards; and
- (c) copies of each Sub-Contract are sent to the Authority immediately after their execution.

F5.5 Unless Approved otherwise, if the total value of the Contract over the Term is, or is likely to be, in excess of [redacted], 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 [redacted];
- (b) within ninety (90) calendar 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 F5.5(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 F5.5(a) includes a full and detailed description of the Sub-Contract opportunity with each of the mandatory fields being completed on Contracts Finder.

F5.6 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.

F5.7 The Authority may from time to time change the format and the content of the information required pursuant to clause F5.6.

F5.8 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.
- F5.9 Notwithstanding clause F5.1, 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 F4.6 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 F5.10 and F5.11.
- F5.10 If the Supplier assigns the right to receive the Price under clause F5.9, the Supplier or the Assignee shall notify the Authority in writing of the assignment and the date upon which the assignment becomes effective.
- F5.11 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.
- F5.12 Clause C1 continues to apply in all other respects after the assignment and shall not be amended without Approval.
- F5.13 Subject to clause F5.14, 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.
- F5.14 Any change in the legal status of the Authority such that it ceases to be a Contracting Authority shall not, subject to clause F5.15, affect the validity of the Contract and the Contract shall bind and inure to the benefit of any successor body to the Authority.
- F5.15 If the rights and obligations under the Contract are assigned, novated or otherwise disposed of pursuant to clause F5.13 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 (Insolvency and Change of Control) and H2 (Termination on Default) 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.

F5.16 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.

F5.17 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.

F6 Change

F6.1 After the Commencement Date, either Party may request a Change subject to the terms of this clause F6. MTR Changes shall be processed in accordance with clause F.7 (MTR Changes).

F6.2 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 12 (Change Control). The Party requesting the Change shall give the other Party sufficient information and time to assess the extent and the effect of the requested Change. The Supplier shall provide an impact and cost statement relating to the proposed Change. If the receiving Party accepts the Change it shall confirm it in writing to the other Party.

F6.3 If the Supplier is unable to accept the Change requested by the Authority or where 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 I1 (Dispute Resolution).

F6.4 A Change takes effect only when it is recorded in a CCN validly executed by both

Parties.

- F6.5 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 (Warranties and Representations).
- F6.6 Clauses F6.6 and F6.7 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.

F7 MTR Changes

- F7.1 The Authority may request MTR Changes by submitting the Change Request Form to the Supplier, provided always that the Authority shall give the Supplier as much notice as reasonably possible of its requirement for MTR Changes.
- F7.2 The Change Request Form for the MTR Changes shall include the following details:
- (a) the proposed MTR policy outcomes to be achieved; and
 - (b) the timescale for completion of the MTR Changes.
- F7.3 If appropriate, depending on the type of MTR policy outcome to be achieved, the Authority may request a series of MTR Changes.
- F7.4 The Supplier shall inform the Authority of any impact on the Services that may arise from the proposed MTR Change(s) and its proposals for mitigating any such impacts.
- F7.5 Unless agreed otherwise, the Supplier shall complete the MTR Changes in the timescale specified in the Change Request Form, and shall promptly notify the Authority when the MTR Changes are completed.
- F7.6 The introduction of MTR Changes will follow the process set out in clause F6(Change) with the exception that they may only be requested by the Authority.

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 D (Statutory Obligations and Corporate Social Responsibility), E1 (Authority Data), E2 (Data Protection and Privacy) or E4 (Confidential Information);
 - (e) any breach of Schedule 6 (Information Assurance and Security); or
 - (f) 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 Subject to clause G1.1 the Supplier's aggregate liability in respect of the Contract does not exceed [Redacted] in the first calendar year of the Contract and for each year thereafter the Price paid or payable in the previous calendar year of the Contract.
- G1.4 Subject to clause G1.1 the Authority's aggregate liability in respect of the Contract does not exceed [Redacted] in the first calendar year of the Contract and for each year thereafter the Price paid or payable in the previous calendar year of the Contract.
- 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 [Redacted] in respect of any one occurrence 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 six (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 three (3) years (or period of existence if the Supplier has not been in existence for three (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.

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 or any third party guaranteeing the obligations of the Supplier under the Guarantee:

- (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 fourteen (14) calendar days of its service) or an application is made for the appointment of a provisional liquidator;
- (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) any event similar to those listed in H1.1(a) to (f) 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 in respect of the Supplier or any third party guaranteeing the obligations of the Supplier under the Guarantee:

- (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, their creditors;
- (b) a petition is presented and not dismissed within fourteen (14) calendar days or order made for their 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 their assets;

- (d) he or any third party guaranteeing the obligations of the Supplier under the Guarantee 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 their assets and such attachment or process is not discharged within fourteen (14) calendar 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 or any third party guaranteeing the obligations of the Supplier under the Guarantee 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 Tax Act 2010 ("**Change of Control**"). The Authority may terminate the Contract with immediate effect by notice and without compensation to the Supplier within six (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 in respect of the Supplier or any third party guaranteeing the obligations of the Supplier under the Guarantee:

- (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;
- (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;
- (c) a receiver, or similar officer is appointed over the whole or any part of its assets;
- (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, its creditors;
- (ii) a petition is presented for its bankruptcy; or
- (iii) a receiver, or similar officer is appointed over the whole or any part of its 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 in respect of the Supplier or any third party guaranteeing the obligations of the Supplier under the Guarantee:

- (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 fourteen (14) calendar 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) any event similar to those listed in clauses H1.5(a) to (f) 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 Termination on 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 twenty (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 ninety (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 C2.1 (Recovery of Sums Due) or to a Force Majeure Event.

H3 Termination on Notice

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

H4 Other Termination 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, 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; or
- (c) the Supplier has not, in performing the Services, complied with its legal obligations in respect of environmental, social or labour law; or
- (d) the Guarantee ceases to be valid or enforceable for any reason (without the Guarantee being replaced with a comparable guarantee to the satisfaction of the Authority with the current guarantor or with another guarantor which is acceptable to the Authority); or
- (e) one of the events described in paragraph 6.1 of Schedule 18 (Financial Distress) take place.

H5 Consequences of Expiry or Termination

H5.1 If the Authority terminates the Contract under clause H2 (Termination on Default) 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 (Termination on Notice) or H4 (Other Grounds) 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 C1 (Payment and VAT), C2 (Recovery of Sums Due), D2 (Fraud and Bribery), E2 (Data Protection and Privacy), E3 (Official Secrets Acts and Finance Act), E4 (Confidential Information), E5 (Freedom of Information), E7 (Intellectual Property Rights), E8 (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), and I12 (Governing Law and Jurisdiction).

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.

- H6.6 The Supplier will document a BCDR Plan, following award of the Contract as set out in Schedule 9 (Business Continuity and Disaster Recovery).

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) immediately vacate any Authority Premises occupied by the Supplier;
 - (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 twenty-one (21) calendar 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 suppliers who have qualified to tender for the future provision of the Services.
- H8.3 The Authority shall require that all potential suppliers 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 the Authority Contract Manager or his nominated representative, to any person representing any potential supplier 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 seven (7) calendar 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 ten (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 H9.12.
- 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 set out in Schedule 2 (Pricing and Payment), Appendices 1 and 2.
- 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 (1) 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.

- H9.5 Upon termination of the Contract for any reason, if there is a Replacement Supplier, the Supplier shall provide all reasonable assistance to the Authority and/or such Replacement Supplier to the extent necessary to effect an orderly transition of the Service.
- H9.6 The cooperation described under clause H9.2 shall include providing to the Authority full access to existing accounts and closed records for seven (7) years to include all reports, collection and enforcement case records, call centre and administration notes on systems and copies of correspondence and Complaints and any other information necessary to achieve an effective transition without disruption to routine operational requirements.
- H9.7 All open and closed records referred to in clause H9.6 shall be transferred back to the Authority on two separate lists on completion or earlier than the termination of the Contract with minimum disruption to routine operational requirements in an agreed accessible/readable format in order that they may be transferred to a Replacement Supplier either:
- (a) upon request; or
 - (b) at expiry or termination of the Contract;
- the closed cases list must show the MAAT reference number, name of Defendant, Outcome and date of closure of case / fulfilment of debt liability.
- H9.8 The Supplier shall not provide final MI performance and KPI reports, including all fully updated case records, less than seven (7) Working Days following the end of the Contract.
- H9.9 The Supplier shall provide an itemised list to the Authority of all warrants and orders, by category, that are in its possession to include details of the issuing court and the stage of execution (application pending, granted, awaiting lapse of appeal period) where the case is still open not less than thirty (30) calendar days prior to the expiry or termination of the Contract.
- H9.10 The Supplier shall also provide separate lists of all Attachment of Earnings applications, Interim Charging Order applications and Final Charging Order applications not yet granted and Final Charging Orders awaiting lapse of appeal period in order to allow the Replacement Supplier to obtain the consent of the issuing court to continue to undertake execution activity as appropriate.
- H9.11 After the confirmed transfer by the Parties of all records and compliance by the Supplier with all obligations contained in this clause H9, all data relating to the Services will be permanently deleted from all Supplier systems, and MI repositories / warehouses within seven (7) calendar days and the Supplier shall inform the Authority CM of the deletion in writing without delay.
- H9.12 The Supplier shall provide a categorised list to the Authority of all warrants and orders,

by category, that are in its possession to include details of the issuing court and stage

of execution (application pending, granted, awaiting lapse of appeal period) no less than thirty (30) calendar days before expiry or termination of the Contract where the case is still open.

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, free of any charge, provide the Authority 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 fifteen (15) Working Days from the date that that request was made.

H11 Financial Distress

The Parties shall comply with the provisions of Schedule 18 (Financial Distress) in relation to Financial Distress of the Supplier and the consequences of a change to their financial standing.

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 twenty (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 ten (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 ten (10) Working Days from the date of the proposal to appoint a Mediator or within ten (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 ten (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 sixty (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 initiate 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 twenty-one (21) calendar 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(a) 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 ten (10) calendar 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 similar 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.

12.6 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 (Termination on Default); 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.

12.7 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.

12.8 Relief from liability for the Affected Party under this clause 12 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.

I3 Notices and Communications

13.1 Subject to clause 13.3, 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.

13.2 If it is not returned as undelivered a notice served in:

- (a) a letter is deemed to have been received two (2) Working Days after the day it was sent; and
- (b) an email is deemed to have been received four (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 earliest.

13.3 Notices pursuant to clauses 11 (Dispute Resolution), 12 (Force Majeure) or 17 (Waiver) 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.

13.4 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]

Address: 102 Petty France, Westminster, London, SW1H 9AJ; and

Email: [Redacted]

(b) For the Supplier:

Contact Name: [Redacted]

Address: [Redacted]

and Email: [Redacted]

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 (Employment) and E7.3 (Intellectual Property Rights) confer benefits on persons named in them (together "**Third Party Provision(s)**") and each person a "**Third Party Beneficiary**") other than the Parties and are intended to be enforceable by Third Party Beneficiaries by virtue of 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 F5 (Change).

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.

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: [Redacted]

Name (block capitals): [Redacted]

Position: [Redacted]

Date: [Redacted]

SIGNED for and on behalf of Advantis
Credit Limited

Signature: [Redacted]

Name (block capitals): [Redacted]

Position: [Redacted]

Date: [Redacted]

Intentionally blank.

SCHEDULE 18 – FINANCIAL DISTRESS

1. DEFINITIONS

1.1. In this Schedule, the following definitions shall apply:

“Accounting Reference Date” means in each year the date to which the Supplier prepares its annual audited financial statements;

“Applicable Financial Indicators” means the financial indicators set out in paragraph 5.1 of this Schedule which are to apply to the Monitored Suppliers as set out in paragraph 5.2 of this Schedule;

“Board” means the Supplier’s board of directors;

“Board Confirmation” means written confirmation from the Board in accordance with paragraph 7 of this Schedule;

“Financial Distress Event Group” or “FDE Group” means the Supplier, Key Sub-contractors, the Guarantor and the Monitored Suppliers;

“Financial Distress Remediation Plan” means a plan setting out how the Supplier will ensure the continued performance and delivery of the Services in accordance with this Contract in the event that a Financial Distress Event occurs. This plan should include what the Authority would need to put in place to ensure performance and delivery of the Services in accordance with this Contract up to and including any insolvency in respect of the relevant FDE Group entity;

“Financial Indicators” in respect of the Supplier, Key Sub-contractors and the Guarantor, means each of the financial indicators set out at paragraph 5.1 of this Schedule, and in respect of each Monitored Supplier, means those Applicable Financial Indicators;

“Financial Target Thresholds” means the target thresholds for each of the Financial Indicators set out at paragraph 5.1 of this Schedule;

“Key Sub-contractors” means any Sub-Contractor which, in the opinion of the Authority, performs (or would perform if appointed) a critical role in the provision of all or any part of the Services. Key Sub-contractors are listed in Schedule 11;

“Monitored Suppliers” means those entities specified at paragraph 5.2 of this Schedule.

2. WARRANTIES AND DUTY TO NOTIFY

2.1. The Supplier warrants and represents to the Authority for the benefit of the Authority that as at the Commencement Date the financial position or, as appropriate, the financial performance of each of the Supplier, Guarantor and Key Sub-contractors satisfies the Financial Target Thresholds.

2.2. The Supplier shall:

- (a) monitor and report on the Financial Indicators for each entity in the FDE Group against the Financial Target Thresholds on a regular basis and in any event, no less than once a year within 120 calendar days after the Accounting Reference Date; and
- (b) promptly notify (or shall procure that its auditors promptly notify) the Authority in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event (and in any event, ensure that such notification is made within 10 Working Days of the date on

which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event).

2.3. Each report submitted by the Supplier pursuant to paragraph 2.2(b) shall:

- (a) be a single report with separate sections for each of the FDE Group entities;
- (b) contain a sufficient level of information to enable the Authority to verify the calculations that have been made in respect of the Financial Indicators;
- (c) include key financial and other supporting information (including any accounts data that has been relied on) as separate annexes;
- (d) be based on the audited accounts for the date or period on which the Financial Indicator is based or, where the Financial Indicator is not linked to an accounting period or an accounting reference date, on unaudited management accounts prepared in accordance with their normal timetable; and
- (e) include a history of the Financial Indicators reported by the Supplier in graph form to enable the Authority to easily analyse and assess the trends in financial performance.

3. FINANCIAL DISTRESS EVENTS

3.1. The following shall be Financial Distress Events:

- (a) an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;
- (b) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity;
- (c) an FDE Group entity committing a material breach of covenant to its lenders;
- (d) a Key Sub-contractor notifying the Authority that the Supplier has not satisfied any material sums properly due under a specified invoice and not subject to a genuine dispute;
- (e) any of the following:
 - (i) commencement of any litigation against an FDE Group entity with respect to financial indebtedness greater than [Redacted] or obligations under a service contract with a total contract value greater than [Redacted];
 - (ii) non-payment by an FDE Group entity of any financial indebtedness;
 - (iii) any financial indebtedness of an FDE Group entity becoming due as a result of an event of default;
 - (iv) the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity; or
 - (v) the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity;

in each case which the Authority reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance and delivery of the Services in accordance with this Contract; and

- (f) any one of the Financial Indicators set out at Paragraph 5 for any of the FDE Group entities failing to meet the required Financial Target Threshold.

- 3.2. The Authority reserves the right to undertake checks by credit rating services to assure itself of the financial viability of any FDE Group entity. Should a credit rating assessment identify concerns in relation to any FDE Group entity, the Authority may consider this to constitute a Financial Distress Event and shall inform the Supplier of the occurrence of such a Financial Distress Event.

4. CONSEQUENCES OF FINANCIAL DISTRESS EVENTS

- 4.1. Immediately upon notification by the Supplier of a Financial Distress Event (or if the Authority becomes aware of a Financial Distress Event without notification and brings the event to the attention of the Supplier, immediately upon bringing such event to the attention of the Supplier), the Supplier shall have the obligations and the Authority shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.
- 4.2. In the event of a late or non-payment of a Key Sub-contractor of the type referred to in Paragraph 3.1(d), the Authority shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier 10 Working Days to:
 - (a) rectify such late or non-payment; or
 - (b) demonstrate to the Authority's reasonable satisfaction that there is a valid reason for late or non-payment.
- 4.3. The Supplier shall (and shall procure that any Monitored Supplier, the Guarantor and/or any relevant Key Sub-contractor shall):
 - (a) at the request of the Authority, meet the Authority as soon as reasonably practicable (and in any event within 3 Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Authority may permit and notify to the Supplier in writing) to review the effect of the Financial Distress Event on the continued performance and delivery of the Services in accordance with this Contract; and
 - (b) where the Authority reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3(a)) that the Financial Distress Event could impact on the continued performance and delivery of the Services in accordance with this Contract:
 - (i) submit to the Authority for its approval, a draft Financial Distress Remediation Plan as soon as reasonably practicable (and in any event, within 10 Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Authority may permit and notify to the Supplier in writing); and
 - (ii) to the extent that it is legally permitted to do so and subject to Paragraph 4.8, provide such information relating to the Supplier, any Monitored Supplier, Key Sub-contractors and/or the Guarantor as the Authority may reasonably require in order to understand the risk to the Services, which may include forecasts in relation to cash flow, orders and profits and details of financial measures being considered to mitigate the impact of the Financial Distress Event.

- 4.4. The Authority shall not withhold its approval of a draft Financial Distress Remediation Plan unreasonably. If the Authority does not approve the draft Financial Distress Remediation Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Remediation Plan, which shall be resubmitted to the Authority within 5 Working Days of the rejection of the first draft. This process shall be repeated until the Financial Distress Remediation Plan is approved by the Authority or referred to the dispute resolution procedure under Paragraph 4.5.
- 4.5. If the Authority considers that the draft Financial Distress Remediation Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not ensure the continued performance of the Supplier's obligations in accordance with the Contract, then it may either agree a further time period for the development and agreement of the Financial Distress Remediation Plan or escalate any issues with the draft Financial Distress Remediation Plan using the dispute resolution procedure under clause I1.
- 4.6. Following Approval of the Financial Distress Remediation Plan by the Authority, the Supplier shall:
- (a) on a regular basis (which shall not be less than fortnightly):
 - (i) review and make any updates to the Financial Distress Remediation Plan as the Supplier may deem reasonably necessary and/or as may be reasonably requested by the Authority, so that the plan remains adequate, up to date and ensures the continued performance and delivery of the Services in accordance with this Contract; and
 - (ii) provide a written report to the Authority setting out its progress against the Financial Distress Remediation Plan, the reasons for any changes made to the Financial Distress Remediation Plan by the Supplier and/or the reasons why the Supplier may have decided not to make any changes;
 - (b) where updates are made to the Financial Distress Remediation Plan in accordance with Paragraph 4.6(a), submit an updated Financial Distress Remediation Plan to the Authority for its Approval, and the provisions of Paragraphs 4.4 and 4.5 shall apply to the review and approval process for the updated Financial Distress Remediation Plan; and
 - (c) comply with the Financial Distress Remediation Plan (including any updated Financial Distress Remediation Plan) and ensure that it achieves the financial and performance requirements set out in the Financial Distress Remediation Plan.
- 4.7. Where the Supplier reasonably believes that the relevant Financial Distress Event under Paragraph 4.1 (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify the Authority and the Parties may agree that the Supplier shall be relieved of its obligations under Paragraph 4.6.
- 4.8. The Supplier shall use reasonable endeavours to put in place the necessary measures to ensure that the information specified at paragraph 4.3(b)(ii) is available when required and on request from the Authority and within reasonable timescales. Such measures may include:
- (a) obtaining in advance written authority from Key Sub-contractors, the Monitored Suppliers and/or the Guarantor authorising the disclosure of the information to the Authority and/or entering into confidentiality agreements which permit disclosure;
 - (b) agreeing in advance with the Authority, Key Sub-contractors, the Monitored Suppliers and/or the Guarantor a form of confidentiality agreement to be entered by the relevant

- parties to enable the disclosure of the information to the Authority;
- (c) putting in place any other reasonable arrangements to enable the information to be lawfully disclosed to the Authority (which may include making price sensitive information available to Authority nominated personnel through confidential arrangements, subject to their consent); and
 - (d) disclosing the information to the fullest extent that it is lawfully entitled to do so, including through the use of redaction, anonymization and any other techniques to permit disclosure of the information without breaching a duty of confidentiality.

5. FINANCIAL INDICATORS

5.1. Subject to the calculation methodology set out at Annex 4 of this Schedule, the Financial Indicators and the corresponding calculations and thresholds used to determine whether a Financial Distress Event has occurred in respect of those Financial Indicators, shall be as follows:

<u>Financial Indicator</u>	<u>Calculation¹</u>	<u>Financial Target Threshold:</u>
1 Return on capital ratio (%)	Earnings before interest, tax, depreciation and amortization (EBITDA) / Capital employed * 100	>6.35
2 Return on assets ratio (%)	EBITDA / total assets *100	>1.60
3 Pre-tax profit (%) or EBITDA ratio	EBITDA / Sales * 100	>4.20
4 Working capital as a percentage of sales Ratio (%)	Working Capital / Sales * 100	>2.85
5 Profitability	EBITDA	Profit (a loss would indicate a Financial Distress Event)
6 Solvency	Total assets less total liabilities	Positive net assets (negative net assets represent a Financial Distress Event)
7 Gearing	(Long term + short term borrowings) / Shareholder equity * 100	<=30
8 Liquidity	(Current assets – Inventory or stock) / Current Liabilities	>1.0
Qualified/ Unqualified accounts	Assessment on whether the Authority can place reliance on the Supplier's financial statements.	Unqualified opinion (qualified opinion, adverse opinion or disclaimer of opinion represents a Financial Distress Event)
Senior personnel involved with insolvency proceedings	Assessment of whether the Supplier's senior personnel are by law in a position to run the company and whether there is a risk of the company could be wound up.	Senior personnel must not be involved with insolvency proceeding (involvement represents a Financial Distress Event)

Key: ¹ – See Annex 1 of this Schedule which sets out the calculation methodology to be used in the calculation of each Financial Indicator.

5.2. Monitored Suppliers

Monitored Supplier	Applicable Financial Indicators [these are the Financial Indicators from the table at 5.1 which are to apply to the Monitored Suppliers]
Lead Supplier: Advantis Credit Limited	All
Parent Company: [Redacted]	All
Ultimate Parent Company: [Redacted]	All

6. TERMINATION RIGHTS

6.1. The Authority shall be entitled to terminate this Agreement under Clause H4 (Other Termination Grounds) if:

- (a) the Supplier fails to notify the Authority of a Financial Distress Event in accordance with Paragraph 2.2(b); and/or
- (b) the Parties fail to agree a Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraphs 4.3 to 4.5; and/or
- (c) the Supplier fails to comply with the terms of the Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with Paragraph 4.6(c).

7. BOARD CONFIRMATION

7.1. Subject to Paragraph 7.4 of this Schedule, the Supplier shall within 120 calendar days after each Accounting Reference Date or within 15 months of the previous Board Confirmation (whichever is the earlier) provide a Board Confirmation to the Authority in the form set out at Annex 2 of this Schedule, confirming that to the best of the Board's knowledge and belief, it is not aware of and has no knowledge:

- (a) that a Financial Distress Event has occurred since the later of the Commencement Date or the previous Board Confirmation or is subsisting; or
- (b) of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event.

7.2. The Supplier shall ensure that in its preparation of the Board Confirmation it exercises due care and diligence and has made reasonable enquiry of all relevant Staff and other persons as is reasonably necessary to understand and confirm the position.

7.3. In respect of the first Board Confirmation to be provided under this Contract, the Supplier shall provide the Board Confirmation within 15 months of the Commencement Date if earlier than the timescale for submission set out in Paragraph 7.1 of this Schedule.

7.4. Where the Supplier is unable to provide a Board Confirmation in accordance with Paragraphs 7.1 to 7.3 of this Schedule due to the occurrence of a Financial Distress Event

or knowledge of subsisting matters which could reasonably be expected to cause a Financial Distress Event, it will be sufficient for the Supplier to submit in place of the Board Confirmation, a statement from the Board of Directors to the Authority setting out full details of any Financial Distress Events that have occurred and/or the matters which could reasonably be expected to cause a Financial Distress Event.

ANNEX 1: CALCULATION METHODOLOGY FOR FINANCIAL INDICATORS

The Supplier shall ensure that it uses the following general and specific methodologies for calculating the Financial Indicators against the Financial Target Thresholds:

General methodology

1. Terminology: The terms referred to in this Annex are those used by UK companies in their financial statements. Where the entity is not a UK company, the corresponding items should be used even if the terminology is slightly different (for example a charity would refer to a surplus or deficit rather than a profit or loss).
2. Groups: Where the entity is the holding company of a group and prepares consolidated financial statements, the consolidated figures should be used.
3. Foreign currency conversion: Figures denominated in foreign currencies should be converted at the exchange rate in force at the relevant balance sheet date.
4. Treatment of non-underlying items: Financial Indicators should be based on the figures in the financial statements before adjusting for non-underlying items.

Specific Methodology

<u>Financial Indicator</u>	<u>Specific Methodology or Description</u>
Return on capital (%)	Assessment of Supplier's profitability and the efficiency with which its capital is employed. EBITDA = Earnings before interest, Tax, Depreciation and Amortisation (EBITDA)
Return on assets (%)	Evaluation of how well management is employing the company's total assets to make a profit. EBITDA = Earnings before interest, Tax, Depreciation and Amortisation (EBITDA)
Pre-tax profit (%)	Assessment of how profitable the Supplier is. EBITDA = Earnings before interest, Tax, Depreciation and Amortisation (EBITDA)

Working capital as % of sales	<p>Calculation of how much the Supplier spends on operational expenses and short-term debt obligations for every [Redacted] of sales.</p> <p>Working capital = current assets / current liabilities or Working capital = (cash + short-term investments + inventory + accounts receivables) / (short-term notes + accounts payables)</p> <p>Working Capital/Sales*100</p>
Return on capital employed (%)	<p>Assessment of Supplier's profitability and the efficiency with which its capital is employed.</p> <p>EBITDA = Earnings before interest, Tax, Depreciation and Amortisation Capital Employed = Total Assets – Current liabilities</p>
Profitability [Redacted]	<p>Assessment of overall profitability.</p> <p>EBITDA = Earnings before interest, Tax, Depreciation and Amortisation</p>
<u>Financial Indicator</u>	<u>Specific Methodology or Description</u>
Solvency [Redacted]	<p>Assessment of available financial resources to deal with adverse trading conditions or legal claims.</p> <p>Solvency = Total Assets – Total Liabilities</p>
Gearing	<p>Assessment on debt used for funding.</p> <p>Long term (over 12 months) + Short term borrowing (repayable within 12 months) / Shareholders equity *100</p>
Liquidity	<p>Assessment of ability to meet short term debts. Where Supplier has a higher than expected gearing ratio, we will consider other ratios like gearing and profitability to assess Supplier's ability to fund its business through existing operations.</p> <p>Current Assets + Inventory or Stock/ Current Liability</p>

Qualified/ Unqualified accounts	Assessment on whether the Authority can place reliance on the Supplier's financial statements.
Senior personnel involved with insolvency proceedings	Assessment of whether the Supplier's senior personnel are by law in a position to run the company and whether there is a risk of the company could be wound up.

ANNEX 2: BOARD CONFIRMATION

Supplier's Name:

Contract Reference Number:

The Board of Directors acknowledge the requirements set out at paragraph 7 of Schedule 18 (Financial Distress) and confirm that the Supplier has exercised due care and diligence and made reasonable enquiry of all relevant Staff and other persons as is reasonably necessary to enable the Board to prepare this statement.

The Board of Directors confirms, to the best of its knowledge and belief, that as at the date of this Board Confirmation it is not aware of and has no knowledge:

a) that a Financial Distress Event has occurred since the later of the previous Board Confirmation and the Commencement Date or is subsisting; or

b) of any matters which have occurred or are subsisting that could reasonably be expected to cause a Financial Distress Event.

On behalf of the Board of Directors:

Chair

Signed

Date

Director

Signed

Date

SCHEDULE 16 – Exit Management

1. DEFINITIONS

- 1.1. Unless the context otherwise requires the following terms shall have the meanings given to them below. Other capitalised terms shall have the meanings given to them in the Terms & Conditions or Schedules in which they first appear.

“Exclusive Assets” means supplier assets (including staff) used exclusively by the supplier or a key subcontractor in the provision of the Services.

“Exit Information” has the meaning given to it in paragraph 3.1 of this Schedule.

“Exit Manager” means the person appointed by each party to manage their respective obligations under this Schedule.

“Exit Plan” means the plan produced and updated by the supplier in accordance with paragraph 4 of this Schedule.

“Non-Exclusive Assets” means Supplier assets (including staff) used by the supplier or a key subcontractor in connection with the Services but which are also used by the Supplier or key subcontractor for other purposes.

Registers” means the register and configuration database referred to in paragraph 2.1 of this Schedule.

“Termination Assistance” means the activities to be performed by the Supplier pursuant to the Exit Plan, and other assistance required by the Authority pursuant to the Termination Assistance Notice.

“Termination Assistance Notice” has the meaning given to it in paragraph 5.1 of this Schedule.

“Termination Assistance Period” means the period specified in a Termination Assistance Notice for which the supplier is required to provide Termination Assistance as such period may be extended pursuant to paragraph 5.2 of this Schedule

“Transferrable Assets” means Exclusive Assets which are capable of legal transfer to the Authority.

“Transferrable Contracts” means sub contracts, licences for Suppliers Software, licences for Third Party Software or other agreements which are necessary to enable the Authority or any replacement Supplier to provide the Services, including in relation to licences, court orders, liability plans and all relevant documentation.

2. READINESS FOR CONTRACT EXIT

- 2.1. During the Contract Period, the Supplier shall:

- 2.1.1. create and maintain a detailed register of all Supplier Assets (including description condition, location and details of ownership and status as either Exclusive Assets or Non-Exclusive Assets) and subcontracts and other relevant agreements required in connection with the Services and;
- 2.1.2. create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Services

- 2.2. The Supplier shall:

- 2.2.1. ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such and

- 2.2.2. procure that all licences for Third Party Software and all subcontracts shall be assignable and/or capable of novation (at no cost or restriction to the Authority) at the request of the Authority, to the Authority (and/or its nominee) and/or a Replacement Supplier upon the Supplier ceasing to provide the Services (or part of them). If the Supplier is unable to do so then the Supplier shall promptly notify the Authority and the Authority may require the Supplier to procure an alternative subcontractor or provider of the Services.
- 2.3. Each party shall appoint an Exit Manager within three (3) months of the Service Commencement Date. The parties Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of this Contract.

3. ASSISTING RE COMPETITION FOR THE SERVICES

- 3.1. The Supplier shall on reasonable notice provide to the Authority and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings) such information (including any access) as the Authority shall reasonably require in order to facilitate the preparation by the Authority or any invitation to tender and/or facilitate any potential Replacement Suppliers undertaking due diligence. (the “**Exit Information**”)
- 3.2. The Supplier acknowledges the Authority may disclose the Suppliers confidential information (excluding the Suppliers or its subcontractors’ prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.
- 3.3. The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Services; and not be disadvantaged in any procurement process compared to the Supplier.

4. EXIT PLAN

- 4.1. The Supplier shall within three (3) months after the Service Commencement Date, deliver to the Authority an Exit Plan which complies with the requirements set out in paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Authority.
- 4.2. The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of the latest date for its submission pursuant to paragraph 4.1 then such Dispute shall be resolved in accordance with the Dispute Resolution procedure.
- 4.3. The Exit Plan shall set out, as a minimum:
 - 4.3.1. a detailed description of both the transfer and cessation processes, including a timetable;
 - 4.3.2. how the Services will transfer to a Replacement Supplier and/or the Authority upon the expiry date ;
 - 4.3.3. details of any contracts which will be available for transfer to the Authority and/or the Replacement Supplier upon the expiry date together with any reasonable costs required to effect such a transfer;
 - 4.3.4. if applicable proposals for the training of key members of the Replacement Supplier’s staff in connection with the continuation of the provision of the Services following the expiry date;
 - 4.3.5. proposals for providing the Authority or a Replacement Supplier copies of all documentation relating to the use and operation of the Services required for their continued use;

- 4.3.6. proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Services;
 - 4.3.7. proposals for the identification and return of all Authority property in the possession of and/or control of the Supplier or any third party
 - 4.3.8. how the Supplier will ensure that there is no disruption to or degradation of the Services during the Termination Assistance Period; and
 - 4.3.9. any other information or assistance reasonably required by the Authority and/or a Replacement Supplier.
- 4.4. The Supplier shall:
- 4.4.1. maintain and update the Exit Plan (and risk management plan) no less frequently than:
 - a) every 12 months throughout the Contract Period and
 - b) no later than twenty (20) Working Days after a request from the Authority for an up to date copy of the Exit Plan;
 - c) as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than ten (10) Working Days after the date of the Termination Assistance Notice
 - d) as soon as reasonably possible following, and in any event no later than twenty (20) Working Days following, any material change to the Services (including all changes under the Change procedure)
 - 4.4.2. jointly review and verify the Exit Plan if required by the Authority and promptly correct any identified failures.
- 4.5. Only if (by notification to the Supplier in writing) the Authority agrees with a draft Exit Plan provided by the Supplier under paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.
- 4.6. A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

5. TERMINATION ASSISTANCE

- 5.1. The Authority shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a "**Termination Assistance Notice**") at least four (4) Months prior to the expiry date or as soon as reasonably practicable (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:
- 5.1.1. the nature of the Termination Assistance required; and
 - 5.1.2. the start date and initial period during which it is anticipated that Termination Assistance will be required.
- 5.2. The Authority shall have an option to extend the Termination Assistance Period beyond the initial period specified in the Termination Assistance Notice in one or more extensions, in each case provided that:
- 5.2.1. no such extension shall extend the Termination Assistance Period beyond the date twelve (12) Months after the initial end date; and
 - 5.2.2. the Authority shall notify the Supplier of any such extension no later than twenty (20) Working Days prior to the date on which the Termination Assistance Period is otherwise due to expire.

- 5.3. The Authority shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier.
- 5.4. In the event that Termination Assistance is required by the Authority but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Authority approved version of the Exit Plan (insofar as it still applies)

6. TERMINATION ASSISTANCE PERIOD

- 6.1. Throughout the Termination Assistance Period the Supplier shall:
- 6.1.1. continue to provide the Services (as applicable) and otherwise perform its obligations under this Contract and, if required by the Authority, provide the Termination Assistance;
 - 6.1.2. provide to the Authority and/or its Replacement Supplier any reasonable assistance and/or access requested by the Authority and/or its replacement supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Services to the Authority and/or its Replacement Supplier;
 - 6.1.3. use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Authority.
 - 6.1.4. subject to paragraph 6.3, provide the Services and the Termination Assistance at no detriment to the Key Performance Indicators (KPIs), the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;
 - 6.1.5. at the Authority's request and on reasonable notice, deliver up-to-date Registers to the Authority;
- 6.2. If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in paragraph 6.1.2 without additional costs to the Authority, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Change Procedure.
- 6.3. If the Supplier demonstrates to the Authority reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular KPIs, the parties shall vary the relevant KPI's and/or the applicable Service Credits accordingly.

7. ASSETS, SUB-CONTRACTS AND SOFTWARE

- 7.1. Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Authority's prior written consent:
- 7.1.1. terminate, enter into or vary any Sub-contract or licence for any software in which, if any, of the Transferable Assets the Authority requires to be transferred to the Authority and/or the Replacement Supplier
 - 7.1.2. which, if any, of:
 - a) the Exclusive Assets that are not Transferable Assets; and
 - b) the Non-Exclusive Assets,

the Authority and/or the Replacement Supplier requires the continued use of; and

- 7.1.3. which, if any, of Transferable Contracts the Authority requires to be assigned or novated to the Authority and/or the Replacement Supplier in order for the Authority and/or its Replacement Supplier to provide the Services from the expiry of the Termination Assistance Period. The Supplier shall provide all reasonable assistance required by the Authority and/or its replacement supplier to enable it to determine which Transferable Assets and Transferable Contracts are required to provide the Services.
- 7.2. Risk in the Transferring Assets shall pass to the Authority or the replacement supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.
- 7.3. Where the Authority and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:
 - 7.3.1. procure a non-exclusive, perpetual, royalty-free licence for the Authority and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which
 - 7.3.2. procure a suitable alternative to such assets, the Authority or the Replacement Supplier to bear the reasonable proven costs of procuring the same.
- 7.4. The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Authority and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Authority reasonably requires to affect this novation or assignment.
- 7.5. The Authority shall:
 - 7.5.1. accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and
 - 7.5.2. once a Transferring Contract is novated or assigned to the Authority and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.
- 7.6. The Supplier shall hold any Transferring Contracts on trust for the Authority until the transfer of the relevant Transferring Contract to the Authority and/or the Replacement Supplier has taken place.
- 7.7. The Supplier shall indemnify the Authority (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Authority (and/or Replacement Supplier) pursuant to paragraph 8.6 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. .
- 8. NO CHARGES**
- 8.1. Unless otherwise stated, the Authority shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

SCHEDULE 15 – IMPLEMENTATION

1. INTRODUCTION

- 1.1 This Schedule defines the process for the preparation and implementation of the Implementation Plan.

2. DEFINITIONS

- 2.1 Unless the context otherwise requires, the following words and expressions shall have the following meanings. Other capitalised terms shall have the meanings given to them in the Terms & Conditions or Schedule in which they first appear:

"Delay"	means: a) a delay in the Achievement of a Milestone by its Milestone Date; or b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan.
"Deliverable Item"	means an item or feature in the supply of the Deliverables delivered or to be delivered by the Supplier at or before a Milestone Date listed in the Implementation Plan.
"Detailed Implementation Plan"	means the detailed plan for the implementation of each of the Services that is developed in accordance with paragraph 3 of this Schedule 15, as amended from time to time in accordance with the Change of Control Procedure set out in clause H1.3 of the Terms & Conditions.
"Draft Implementation Plan"	means the plan for the implementation of the Services contained in Annex 1 of this Schedule 15.
"Implementation Period"	has the meaning given to it in paragraph 7.1
"Implementation Plan"	means the Draft Implementation Plan or (if and when approved by the Authority pursuant to paragraph 3 of this Schedule 15) the Detailed Implementation Plan as updated from time to time in accordance with paragraph 4.1.
"Implementation Services"	means the services set out in the Implementation Plan.
"Milestone Date"	means the date set against the relevant Milestone in the Implementation Plan by which the Milestone shall be completed.
"Milestone"	means an event or task described in the Implementation Plan which, if applicable, shall be completed by the relevant Milestone Date.

3. **AGREEING AND FOLLOWING THE IMPLEMENTATION PLAN**

- 3.1 A Draft Implementation Plan, as provided as part of the Tender response, is set out in the Annex to this Schedule. The Supplier shall provide a Detailed Implementation Plan no later than 10 Working Days after the Commencement Date.
- 3.2 The Detailed Implementation Plan must:
- 3.2.1 clearly outline all the Implementation Services to be delivered by the Supplier in the Implementation Period;
 - 3.2.2 clearly outline the required roles and responsibilities of both Parties, including staffing requirements;
 - 3.2.3 incorporate the Supplier's proposed timescales and methodology for completing the Implementation Plan prior to the Service Commencement Date; and
 - 3.2.4 provide confidence to the Authority that the Supplier will be ready to deliver the provision of the Services on and from the Service Commencement Date.
- 3.3 The Authority will provide comments on the Supplier's Draft Implementation Plan no later than the Commencement Date.
- 3.4 Prior to the submission of the Detailed Implementation Plan to the Authority, the Authority shall have the right:
- 3.4.1 to review any documentation produced by the Supplier in relation to the development of the Detailed Implementation Plan; and
 - 3.4.2 to require the Supplier to include any reasonable changes or provisions in the Detailed Implementation Plan.
- 3.5 Following receipt of the Detailed Implementation Plan, the Authority shall:
- 3.5.1 review and comment on the Detailed Implementation Plan as soon as reasonably practicable; and
 - 3.5.2 notify the Supplier in writing that it approves or rejects the Detailed Implementation Plan no later than 20 Working Days after the date on which the Detailed Implementation Plan is delivered to the Authority.
- 3.6 If the Authority rejects the Detailed Implementation Plan, the Supplier shall revise the Detailed Implementation Plan and re-submit a revised Detailed Implementation Plan to the Authority for the Authority's Approval within 10 Working Days of the date of the Authority's notice of rejection.
- 3.7 If the Authority rejects the re-submitted Detailed Implementation Plan, the Supplier's Contract Manager shall meet with the Authority within 10 Working Days of the rejection for the purposes of agreeing the Detailed Implementation Plan.
- 3.8 If the Detailed Implementation Plan is not agreed within 5 Working Days of the meeting pursuant to paragraph 3.7, the matter shall be referred to the Supplier and Authority's Commercial Contract Manager who shall act reasonably and in good

faith to agree the Detailed Implementation Plan as soon as reasonably practicable and in any event, within 10 Working Days.

3.9 In the event that the persons appointed under paragraph 3.8 are unable to agree the Detailed Implementation Plan, then the matter shall be dealt with as a Dispute and such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

3.10 Once approved by the Authority or agreed or determined in accordance with paragraphs 3.6 to 3.9 above, the Detailed Implementation Plan shall replace the Draft Implementation Plan from the date of the Authority's notice of Approval or the date on which the Detailed Implementation Plan is agreed or determined.

3.11 The Supplier shall provide each of the Deliverable Items identified in the Implementation Plan by the date assigned to that Deliverable Item in the Implementation Plan so as to ensure that each Milestone identified in the Implementation Plan is achieved on or before its Milestone Date.

3.12 The Supplier shall monitor its performance against the Implementation Plan and Milestones (if any) and report to the Authority on such performance.

4. REVIEWING AND CHANGING THE IMPLEMENTATION PLAN

4.1 Subject to Paragraph 4.3, the Supplier shall keep the Implementation Plan under review in accordance with the Authority's instructions and ensure that it is updated on a regular basis.

4.2 The Authority shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.

4.3 Changes to any Milestones, shall only be made in accordance with the Change procedure.

4.4 Time in relation to compliance with the Implementation Plan shall be of the essence and failure of the Supplier to meet a Milestone (including the relevant Milestone Date) shall be a material breach of this Contract.

5. WHAT TO DO IF THERE IS A DELAY

5.1 If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay under this Contract it shall:

5.1.1 notify the Authority as soon as practically possible and no later than within two (2) Working Days from becoming aware of the Delay or anticipated Delay;

5.1.2 include in its notification an explanation of the actual or anticipated impact of the Delay;

5.1.3 comply with the Authority's instructions in order to address the impact of the Delay or anticipated Delay; and

5.1.4 use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay.

- 5.2 Any disputes about or arising out of Delays shall be resolved through the Dispute Resolution Procedure set out in Clause I1 (Dispute Resolution) of the Terms & Conditions. Pending the resolution of the dispute, both Parties shall continue to work together to resolve the causes of, and mitigate the effects of, the Delay.

6. IMPLEMENTATION PERIOD

- 6.1 The Implementation Period will be a minimum of 5-month, 2-week period.

- 6.2 During the Implementation Period, the Outgoing Supplier shall retain full responsibility for all existing services until the Service Commencement Date or as otherwise formally agreed with the Authority. The Supplier's full-service obligations shall formally be assumed on the Service Commencement Date.

- 6.3 The Supplier shall:

- 6.3.1 perform each of the tasks identified in the Implementation Plan by the applicable Milestone Date assigned to the particular task in the Implementation Plan;
- 6.3.2 work cooperatively and in partnership with the Authority and Outgoing Supplier to understand the scope of Services to ensure a mutually beneficial handover of the Services;
- 6.3.3 co-operate with the Authority in connection with the transition and migration of any of the Authority's Data that is in the possession of the Authority or the Outgoing Supplier to the Supplier, and in all other respects, such that there is a seamless transition of the responsibility of providing the Services from the Outgoing Supplier with minimal disruption;
- 6.3.4** liaise with the Outgoing Supplier to enable the full completion of the Implementation Period activities

- 6.4** In addition, the Supplier shall:

- 6.4.1 manage and report progress against the Implementation Plan;
- 6.4.2 construct and maintain an implementation risk register and issue register in conjunction with the Authority detailing how risks and issues will be effectively communicated to the Authority in order to mitigate them;
- 6.4.3 attend progress meetings (frequency of such meetings shall be agreed before the start of the Implementation Period) in accordance with the Authority's requirements during the Implementation Period. Implementation meetings shall be chaired by the Authority and all meeting minutes shall be kept and published by the Supplier; and
- 6.4.4 ensure that all risks associated with the Implementation Period are minimised to ensure a seamless change of control between the Outgoing Supplier and the Supplier.

ANNEX 1 – IMPLEMENTATION PLAN

[Redacted]

SCHEDULE 14 – POLICIES AND STANDARDS

1. INTRODUCTION

- 1.1 The Supplier shall at all times comply with the Policies and Standards listed in Annex 1 of this Schedule.
- 1.2 The Parties acknowledge that any standard, policy and/or other document referred to within a Policy or Standard shall be deemed to form part of that Policy or Standard.

2. GENERAL

- 2.1 The Authority shall provide copies of the Policies and Standards from time to time to the Supplier upon request.
- 2.2 Throughout the Contract Period, the Parties shall monitor and notify each other of any new or emergent policies or standards which could affect the Suppliers provision, or the Authority's receipt, of the Services.
- 2.3 Where a new or emergent standard is to be developed or introduced by the Authority, the Supplier shall be responsible for ensuring that the potential impact on the Suppliers provision, or the Authority's receipt, of the Services is explained to the Authority (in a reasonable timeframe), prior to the implementation of the new or emergent standard.
- 2.4 Where new versions of the Authority's Policies or Standards are developed and notified to the Supplier, the Supplier shall be responsible for ensuring that the potential impact on the Suppliers provision, or the Authority's receipt, of the Services is explained to the Authority (in a reasonable timeframe), prior to the implementation of the new version of the Policy or Standard, and the Supplier shall comply with such revised Policy or Standard (and any necessary Variations to the Contract shall be agreed in accordance with clause F4 (Change)).

3. CONFLICTING POLICIES OR STANDARDS


Where Policies or Standards referenced conflict with each other or with Good Industry Practice, then the later Policy or Standard or best practice shall be adopted by the Supplier. Any such alteration to any Policy or Standard(s) shall require the prior written agreement of the Authority and shall be implemented within an agreed timescale.

ANNEX 1

POLICES AND STANDARDS

<u>Policy or Standard</u>	<u>Description</u>
Anti-Slavery Policy	The policy will be set out in the relevant modern slavery statements and Government reports published from time to time.
APIs and System Integration Standard	https://www.gov.uk/guidance/gds-api-technical-and-data-standards
Authority's Complaints Procedure	https://www.gov.uk/government/organisations/legal-aid-agency/about/complaints-procedure
British Standard 7858	https://www.bsigroup.com/en-GB/search-results/?q=7858&Page=1&tab=Standards
British Standard 8555	https://www.bsigroup.com/en-GB/search-results/?q=8555&Page=1&tab=All
Centre for the Protection of National Infrastructure (CPNI) Standard for Secure Destruction of Sensitive Items	https://www.cpni.gov.uk/secure-destruction-0
Civil Service – Good Governance	https://www.gov.uk/government/publications/corporate-governance-code-for-central-government-departments-2017
Civil Service Code	Civil service conduct and guidance - GOV.UK (www.gov.uk)
Cyber Essentials Scheme Overview	https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
Minimum Cyber Security Standard	https://www.gov.uk/government/publications/the-minimum-cyber-security-standard
Ministry of Justice (MoJ) Cyber and Technical Security Guidance	Security Guidance (justice.gov.uk)
Supplier Assurance Questions	https://www.ncsc.gov.uk/guidance/supplier-assurance-questions
Government's 10 Steps to Cyber Security	https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
Digital Service Standard	https://www.gov.uk/service-manual/service-standard
Disclosure Barring Service (DBS) Checks	https://www.gov.uk/disclosure-barring-service-check/overview
Email Security Standard	https://www.gov.uk/government/publications/email-security-standards
FCA Principles of Business and Consumer Credit Rulebook	https://www.handbook.fca.org.uk/handbook/PRIN/2/1.html
Federal Information Processing Standard (FIPS) 140-3	https://csrc.nist.gov/publications/detail/fips/140/3/final
Government Baseline Personnel Security Standard (BPSS)	https://www.gov.uk/government/publications/government-baseline-personnel-security-standard
Government (Cabinet Office and NCSC) guidance on Security Technology at OFFICIAL	https://www.gov.uk/government/collections/securing-technology-at-official .

<u>Policy or Standard</u>	<u>Description</u>
Government Buying Standards	https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs
Government Digital Service Standards	GDS API Technical and Data Standards page.
Government Functional Standard GovS 007: Security	https://www.gov.uk/government/publications/government-functional-standard-govs-007-security
Government Security Classifications (Data Security)	Government Security Classifications - GOV.UK (www.gov.uk)
Government Security Policy Framework	https://www.gov.uk/government/collections/government-security
Greening Government Commitments	https://www.gov.uk/government/collections/greening-government-commitments
Health & Safety Policy	[Redacted]
HMT's Financial Reporting Manual	2021-22_FReM - Dec_21.pdf (publishing.service.gov.uk)
Open Standards for Government	https://www.gov.uk/government/publications/open-standards-for-government
ISO 14001	https://www.iso.org/standard/60857.html
ISO/IEC 20000	https://www.iso.org/search.html?q=20000
ISO 22301	https://www.iso.org/search.html?q=22301&hPP=10&idx=all_en&p=0
ISO/IEC 27001	ISO - ISO/IEC 27001 and related standards — Information security management
ISO/IEC 27002	https://www.iso.org/standard/75652.html
LAA Departmental Retention Periods	Record retention and disposition schedules - GOV.UK (www.gov.uk)
Legal Aid Means Test Review	https://www.gov.uk/government/consultations/legal-aid-means-test-review
Ministry of Justice Data Sharing Principles	https://mojdigital.blog.gov.uk/2016/10/06/data-principles-the-right-ingredients-to-solving-the-data-spaghetti-problem/
MoJ Code of Conduct	[Redacted]
National Cyber Security Centre Assured Service Service Requirement Sanitisation Standard	Secure sanitisation of storage media - NCSC.GOV.UK
National Cyber Security Centre (CHECK scheme)	https://www.ncsc.gov.uk/guidance/penetration-testing
National Cyber Security Centre Cloud Security Guidance	https://www.ncsc.gov.uk/guidance/cloud-security-collection
National Cyber Security Centre Cloud Security Principles	The cloud security principles - NCSC.GOV.UK

<u>Policy or Standard</u>	<u>Description</u>
National Cyber Security Centre End User Devices Platform Security Guidance	Device Security Guidance - NCSC.GOV.UK
National Cyber Security Centre (end-user device reset procedures)	https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/erasing-devices
National Cyber Security Centre (guidance)	https://www.ncsc.gov.uk/section/advice-guidance/all-topics
National Cyber Security Centre (risk management)	https://www.ncsc.gov.uk/collection/risk-management-collection
National Cyber Security Centre (secure sanitisation of storage media)	https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media
National Standards for Enforcement Agencies	https://www.gov.uk/government/publications/bailiffs-and-enforcement-agents-national-standards
Payment Card Industry PCI Data Security Standard	https://www.pcisecuritystandards.org/
Protective Monitoring	Security policy framework: protecting government assets - GOV.UK (www.gov.uk)
Public Sector Equality Duty	Public sector equality duty - GOV.UK (www.gov.uk)
Supplier Code of Conduct	Supplier Code of Conduct - v2 (publishing.service.gov.uk)
Technical Controls Summary (technical and security controls recommended by Cabinet Office)	https://www.gov.uk/government/collections/securing-technology-at-official
UK HMG Technology Code of Practice	https://www.gov.uk/guidance/the-technology-code-of-practice
Welsh Language Scheme	 welsh-language-scheme-web.pdf

SCHEDULE 13 – GOVERNANCE AND CONTRACT MANAGEMENT

1. INTRODUCTION

- 1.1. The Parties acknowledge that successful delivery of the Services and the Contract depends upon effective management by the Authority and the Supplier, and the Supplier acknowledges that the Authority places a high importance on contract management. This Schedule outlines the means by which the Authority and the Supplier shall each discharge their respective governance functions and obligations under the Contract. For the avoidance of doubt, nothing in this Schedule 13 (including the participation of the Authority in any governance board) shall operate so as to fetter the rights of the Authority to make decisions and/or exercise its rights or discretion under the Contract.

2. AUTHORITY'S MANAGEMENT STRUCTURE

- 2.1. The Authority shall appoint:
- a) a Commercial Contract Manager (CCM) who will be responsible for the overall commercial contract management of this Contract;
 - b) a Senior Business Owner (SBO) who will be responsible for the overall operational management of this Contract;
 - c) an Authority Contract Manager (ACM) who will be responsible for the overall contract management of this Contract;
 - d) a Finance Officer (FO) who will be responsible for the overall financial management of this Contract;
 - e) a Cyber Security Officer (CSO) who will be responsible for oversight of Security Plan for this Contract.
- 2.2. Should the Authority's management structure change throughout the Contract Period, the Supplier will be expected to be flexible and work in partnership with the Authority in respect of any such changes.

3. SUPPLIER'S MANAGEMENT STRUCTURE

- 3.1. The Supplier shall ensure it has adequate internal management structures in place to manage the Contract from the Commencement Date.
- 3.2. The Supplier shall nominate a Supplier Contract Manager (SCM) who shall be the single point of contact for the Authority and who shall have overall responsibility for the Supplier's management of the Contract.
- 3.3. Where the nominated CM is being replaced, the Supplier shall appoint a suitably qualified person of equivalent experience as soon as possible and shall ensure any proposed change does not adversely affect the smooth operation of the Contract.
- 3.4. The Supplier shall, by the Commencement Date have a clear internal mechanism in place for dealing with any issues relating to the Contract and/or the Services and have a clear escalation process and provide the Authority with a clear and sufficiently detailed description of this mechanism by the Commencement Date.

4. CONTRACT GOVERNANCE

- 4.1. The Supplier shall ensure that the CM attends the following meetings in accordance with the schedule of meetings set out in paragraph 4.8:

- a) Management information meeting (as described in paragraph 4.2)
- b) Service review/contract management meeting (as described in paragraph 4.3)
- c) Quarterly security group meeting (as described in paragraph 4.4);
- d) Annual contract review meeting (as described in paragraph 4.5).

4.2. The remit of the management information meeting shall include:

- a) review of all MI and financial reports for accuracy;
- b) understanding issues and trends from MI and financial data;
- c) sharing opportunities for efficiencies, continuous improvement and innovation in the way MI and finance reports are provided.

4.3. The remit of the service review/contract management meeting shall include:

- a) monitoring the Supplier's compliance with its obligations under the Contract;
- b) monitoring the Supplier's delivery of the Implementation Plan;
- c) review and monitoring of the Supplier's delivery and performance of the operational services, including complaints, risks, and issues;
- d) review of any commercial aspects of the Contract;
- e) addressing issues, trends, and developments in relation to the delivery of the implementation plan and/or the Services;
- f) sharing best practice and details of relevant initiatives;
- g) sharing opportunities for efficiencies, continuous improvement, and innovation;
- h) forward planning.

4.4. The remit of the security working group shall include:

- a) addressing security incidents and reviewing actions taken by the Supplier to mitigate
- b) addressing risk and vulnerabilities Rectification Plans and reviewing updates.
- c) reviewing IT patching updates and issues
- d) reviewing and addressing annual IT Health Check results, rectification plans, updates on forward plans/scope of future testing
- e) sharing best practice on Data Protection and GDPR and reviewing issues
- f) sharing best practice on Protective Measures and reviewing issues
- g) reviewing updates on Supplier staff vetting processes and issues
- h) reviewing risks and compliance with Schedules 6 and 10.

4.5. The remit of the Annual Contract Review meeting shall include:

- a) monitoring the Suppliers compliance with its obligations under the Contract;
- b) highlighting key successes and lessons learned from the previous 12 months;
- c) agreeing a forward-looking approach for the subsequent 12 months;
- d) discussion of annual trends, complaints, risks, and issues;
- e) assessing the relationship between the parties and the current/new ways of working;

- f) reviewing any commercial aspects of the Contract;
 - g) reviewing and agreeing any variations and changes to prices, performance measure and targets.
- 4.6. The meeting organiser will arrange for minutes to be taken at any of the meetings listed above and for the minutes to be promptly circulated after each meeting.
- 4.7. Unless otherwise agreed between the Parties, the agenda for all meetings shall be prepared and circulated ahead of the date of the relevant meeting.
- 4.8. The Supplier is responsible for providing management information and reports in advance of the meetings in accordance with the requirements of Schedule 8 – Performance, Management Information and Reporting.
- 4.9. The attendees and meeting frequency of each of the above meetings is set out below. In addition to the Supplier representatives listed below, the Authority may, acting reasonably, require other Supplier Staff to attend meetings from time to time, including senior representatives of the Supplier's business.

Meeting Name	Who	Frequency
Management Information Meeting	ACM, SCM, FO	Monthly The ACM will chair all meetings and be responsible for secretariat responsibilities.
Service Review/Contract Management meeting	ACM, CCM, SCM, FO	Two weekly during the implementation period Monthly following service commencement with additional meetings as required by the Authority The ACM will chair all meetings and be responsible for secretariat responsibilities.
Security Working Group	ACM, SCM, CSO	Quarterly following service commencement with additional meetings as required by the Authority. The ACM will chair all meetings and be responsible for secretariat responsibilities.
Annual Contract Review Meeting	SBO, ACM, CCM, FO, SCM	Annual The SBO will chair all meetings and be responsible for secretariat responsibilities

SCHEDULE 12 - CHANGE CONTROL FORMS

Change Request Form

(For completion by the Party requesting the Change)

Contract Title:	Party requesting Change:
Name of Supplier: Advantis Credit Limited	
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: Advantis Credit Limited			
Change Number:			
Date on which Change takes effect:			
Contract between: The Lord Chancellor and Advantis Credit Limited			
It is agreed that the Contract is amended, in accordance with Regulation 72 of the Public Contracts Regulations 2015, as follows:			
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 Lord Chancellor		Signed for and on behalf of Advantis Credit Limited	
Signature		Signature	
Name		Name	
Title		Title	
Date		Date	

SCHEDULE 11 – APPROVED SUB-CONTRACTORS

The Supplier is entitled to sub-contract its obligations under this Contract to the approved Sub-contractors listed in the table below.

[Redacted]

SCHEDULE 10 – DATA PROCESSING

1. GENERAL

- 1.1. This Schedule shall be completed by the Controller, who may take account of the view of the Processor, however the final decision as to the content of this Schedule shall be with the Controller at its absolute discretion.
- 1.2. The contact details of the Authority's Data Protection Officer are:
Email: [Redacted]
Address: [Redacted]
Ministry of Justice
[Redacted]
102 Petty France
London
SW1H 9AJ
- 1.3. The contact details of the Supplier's Data Protection Officer are:
Email: [Redacted]
Address: [Redacted]
- 1.4. The Supplier shall comply with any further written instructions with respect to processing by the Authority.
- 1.5. Any such further instructions shall be incorporated into this Schedule 10.

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of Data Protection Legislation, the Authority is the Controller and the Supplier is the Processor in accordance with Clause 1.1.
Subject matter of the processing	The Authority provides civil and criminal legal aid in England and Wales to help people deal with their legal problems and processes Personal Data in respect of these. In addition, the Authority processes Personal Data regarding its employees and key contacts at suppliers and third parties. The Supplier is providing debt and enforcement collection services for those people who are determined, by the Authority or by the Supplier, to have a criminal legal aid contribution, including decision making by the Supplier that such a contribution is not due.
Duration of the processing	Data regarding the management of the Contract will be processed for the duration of the Term including any Extensions of the Contract, and for a further period of 6 years following the end of the Contract. Personal Data regarding individual cases will be kept for a period up to 7 years from the date of the final bill being paid by the Authority, or any debt or contribution amount being paid in full, whichever is later. Where such period exceeds the Term, the Personal Data will be transferred in accordance with exit provisions in this Contract and not retained. Personal Data in Complaints Logs will be stored for the current Financial year in which the complaint is resolved and then one further year.

Description	Details
	<p>The Supplier shall seek permission from the Authority before destroying Personal Data in accordance with the retention periods.</p>
<p>Nature and purposes of the processing</p>	<p>Personal Data relating to Staff and Authority staff will be processed for the purposes of contract management activity relating to this Contract and the provision of Services under this Contract.</p> <p>Personal Data relating to Authority staff and Staff, legal aid clients and their partners, legal aid providers and other related individuals to proceedings will be Processed in accordance with the Authority's written reasonable instructions to provide the Services and undertake the following processing activities:</p> <ul style="list-style-type: none"> ● set up and manage debt accounts with personal information; ● record personal information, monies received and debt balances and issue notifications regarding debt; ● carry out both outgoing and incoming telephone calls and record voice conversations; ● take payments via industry standard methods of payment; ● carry out enforcement of debt including use of Enforcement Agents and bailiffs for personal visits; ● carry out K&E Checks; ● administer and issue CCOs; ● use third-party systems to trace debtors i.e. Equifax; and ● retain Personal Data for up to 7 years after the date the final bill is paid or the date the debt is cleared in full, whichever is the later. <p>The lawful basis for processing Personal Data relating to individual legal aid cases is performance of a public task, specifically the responsibility of the Authority set out in the Legal Aid, Sentencing and Punishment of Offenders Act 2012 as delegated to the Supplier as the Service.</p> <p>The Ministry of Justice is an official Authority for the purposes of processing Criminal Offence Data and the Supplier is an agent for this processing.</p> <p>The Article 9 condition for processing Special Category Data is substantial public interest and the substantial public interest condition is statutory and governmental purposes, specifically the functions of the Authority set out in the Legal Aid, Sentencing and Punishment of Offenders Act 2012 for which the Supplier is acting as an agent of the Authority.</p>
<p>Type of Personal Data being Processed</p>	<p>To complete the purposes defined above the Supplier will process Personal Data about Legal Aid clients, partners and other relevant individuals including children's data, specifically:</p> <ul style="list-style-type: none"> ○ Legal Aid reference numbers; ○ Full name of debtor and partner; ○ Home address of debtor and partner; ○ Prison address of debtor; ○ Business address of debtor; ○ Date of birth of debtor; ○ Gender of debtor; ○ Marital status of debtor ○ NI number of debtor;

Description	Details
	<ul style="list-style-type: none"> ○ Telephone number(s) of debtor; ○ Email address of debtor; ○ Any Personal Data voluntarily disclosed by the debtor or with whom the Supplier and other Sub-Contracted agents communicates; in relation to their financial circumstances, vulnerability circumstances and ability to pay their debts; and <p>Details of individual legal aid clients and (where relevant) their partner's financial circumstances which may include:</p> <ul style="list-style-type: none"> ○ bank account numbers, sort code and account balances; ○ details of financial transactions; ○ details of employment status and employer's address; ○ details of benefit claims and financial support and assistance; ○ details of debts; and ○ details of property, vehicles and other capital assets such as savings, stocks and shares. <p>Details of legal aid providers including:</p> <ul style="list-style-type: none"> ○ name(s) of staff members; ○ business email addresses of provider staff members; ○ business phone numbers of provider staff members; and ○ account numbers (unique identifiers) for provider staff members. <p>Details of Authority staff including:</p> <ul style="list-style-type: none"> ○ names; ○ business email addresses; and ○ usernames. ○ Audit records detailing actions taken on the Authority's System. <p>To complete the purposes defined above the Supplier will process Criminal Offence Data relating to legal aid clients and other parties in criminal proceedings including:</p> <ul style="list-style-type: none"> ○ nature and type of case; ○ court hearing the case and hearing dates; ○ Outcome of proceedings; and ○ Details of penalties in criminal proceedings, in particular whether a legal aid client is imprisoned. <p>Special Category Data: The following types of Special Category Data may be processed in respect of individual legal aid clients, their partners, children, and other individuals associated with Criminal Court proceedings:</p> <ul style="list-style-type: none"> ○ Personal Data concerning health; <p>Special Category Data relating to the following may be processed only where this information is indirectly inferred from offence or court details or disclosed by the Data Subject directly to the Authority or Supplier:</p> <ul style="list-style-type: none"> ○ Personal Data concerning a person's sex life; and ○ Personal Data concerning a person's sexual orientation.

Description	Details
Categories of Data Subject	<ul style="list-style-type: none"> • Authority staff and Staff • Legal Aid clients • Partners and other associated individuals of Legal Aid clients • Legal Aid providers • Other parties involved in proceedings relating to Legal Aid clients.
International transfers and legal gateway	Personal Data will only be processed in the UK
<p>Plan for return and destruction of the data once the processing is complete</p> <p>Unless requirement under union or member state law to preserve that type of data</p>	<p>See the 'Duration' box above. Before termination or expiry of the Contract, the Supplier shall securely destroy or return to the Authority all the Authority's Personal Data in its possession or control. When Personal Data is destroyed or removed from the Supplier System, the Supplier is required to produce a data destruction certificate or other written assurance that this has taken place. This requirement shall not apply to the extent that the Supplier is required by applicable Law to retain some or all the Authority's Personal Data, or to retain the Authority's Personal Data it has archived on back-up systems, which the Supplier shall securely isolate and protect from any further processing except to the extent required or permitted by such Law.</p>

SCHEDULE 9 – BUSINESS CONTINUITY AND DISASTER RECOVERY

1. PURPOSE

- 1.1 This Schedule sets out the Authority's requirements for ensuring continuity of the business processes and operations supported by the Services in circumstances of disruption or failure, and for restoring the Services through business continuity and, as necessary, disaster recovery procedures. It also includes the requirement on the Supplier to develop, review, test, change and maintain a BCDR Plan.

2. DEFINITIONS

- 2.1 Unless the context otherwise requires the following terms shall have the meanings given to them below. Other capitalised terms shall have the meanings given to them in the Terms & Conditions or Schedules in which they first appear.

"BCDR Plan Review Report" has the meaning given to it in Paragraph 7.2 (Review and Amendment of the BCDR Plan) of this Schedule.

"Business Continuity Plan" has the meaning given to it in Paragraph 3.2(b) (BCDR Plan) of this Schedule.

"Business Continuity Services" means as it is described in paragraph 5.2(b) of this Schedule.

"Disaster" means the occurrence of one or more events which either separately or cumulatively, mean that the Services, or a material part of the Services, will be, or are reasonably anticipated to be, unavailable for more than 24 hours during Extended Business Hours.

"Disaster Recovery Plan" has the meaning given to it in Paragraph 3.2(c) (BCDR Plan) of this Schedule.

"Extended Business Hours" means 8am to 10pm, Sunday to Saturday.

"Senior Information Risk Owner" means the Authority's senior information risk owner.

3. BCDR PLAN

- 3.1 Within twenty (20) Working Days of the Commencement Date the Supplier shall prepare and deliver to the Authority for its Approval, a plan (being the **"BCDR Plan"**) which shall detail the processes and arrangements that the Supplier shall follow to:

- (a) ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Services; and
- (b) the recovery of the Services in the event of a Disaster.

- 3.2 The BCDR Plan shall be divided into 3 parts:

- (a) Part A which shall set out general principles applicable to the BCDR Plan;
- (b) Part B, which shall relate to business continuity (the "**Business Continuity Plan**"); and
- (c) Part C, which shall relate to Disaster recovery (the "**Disaster Recovery Plan**");

which shall, unless otherwise required by the Authority in writing, be based upon and be consistent with the provisions of Paragraphs 4, 5 and 6 of this Schedule 9 and cover all components of the Services.

3.3 Following receipt of the draft BCDR Plan from the Supplier, the Authority shall:

- (a) review and comment on the draft BCDR Plan as soon as reasonably practicable; and
- (b) notify the Supplier in writing that it approves or rejects the draft BCDR Plan no later than 20 Working Days after the date on which the draft BCDR Plan is first delivered to the Authority.

3.4 If the Authority rejects the draft BCDR Plan:

- (a) it shall inform the Supplier in writing of the reasons for rejection; and
- (b) the Supplier shall then revise the draft BCDR Plan (taking reasonable account of the Authority's comments) and shall re-submit a revised draft BCDR Plan to the Authority for the Authority's Approval within 20 Working Days of the date of the Authority's notice of rejection. The provisions of Paragraph 3.3 (BCDR Plan) above and this Paragraph 3.4 shall apply again to any resubmitted draft BCDR Plan, provided that either Party may refer any disputed matters for resolution in accordance with Clause I1 (Dispute Resolution) at any time.

4. **PART A: GENERAL PRINCIPLES AND REQUIREMENTS**

4.1 Part A of the BCDR Plan shall:

- (a) set out how the Business Continuity Plan and the Disaster Recovery Plan link to each other;
- (b) provide details of how the invocation of any element of the BCDR Plan may affect the operation of the Services and any services provided to the Authority by other suppliers;
- (c) contain an obligation upon the Supplier to liaise with the Authority and (at the Authority's request) any other suppliers with respect to issues concerning business continuity and disaster recovery where applicable;
- (d) detail how the BCDR Plan links and interoperates with any overarching and/or connected disaster recovery plan or business continuity plan of the Authority and any of its other suppliers in each case as notified to the Supplier by the Authority from time to time;

- (e) contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multi-channels (including but without limitation a web-site (with FAQs), e-mail, phone and fax) for both portable and desk top configurations, where required by the Authority;
- (f) contain a risk analysis, including:
 - (i) failure or disruption scenarios and assessments and estimates of frequency of occurrence;
 - (ii) identification of any single points of failure within the Services and processes for managing the risks arising therefrom;
 - (iii) identification of risks arising from the interaction of the Services with the services provided by other suppliers; and
 - (iv) a business impact analysis (detailing the impact on business processes and operations) of different anticipated failures or disruptions;
- (g) provide for documentation of processes, including business processes, and procedures;
- (h) set out key contact details (including roles and responsibilities) for the Supplier (and any Sub-Contractors) and for the Authority;
- (i) identify the procedures for reverting to "normal service";
- (j) set out method(s) of recovering or updating Authority Data collected (or which ought to have been collected) during a failure or disruption to ensure that there is no data loss and to preserve data integrity;
- (k) identify the responsibilities (if any) that the Authority has agreed it will assume in the event of the invocation of the BCDR Plan; and
- (l) provide for the provision of technical advice and assistance to key contacts at the Authority as notified by the Authority from time to time to inform decisions in support of the Authority's business continuity plans.

4.2 The BCDR Plan shall be designed so as to ensure that:

- (a) the Services are provided in accordance with the Contract at all times during and after the invocation of the BCDR Plan;
- (b) the adverse impact of any Disaster, service failure, or disruption on the operations of the Authority is minimal as far as reasonably possible;
- (c) it complies with the relevant provisions of ISO/IEC 27002 (as amended), ISO 22031 and all other industry standards from time to time in force;
- (d) there is a process for the management of Disaster recovery testing detailed in the BCDR Plan; and

- (e) it is upgradeable and sufficiently flexible to support any changes to the Services or to the business processes facilitated by and the business operations supported by the Services.
- 4.3 The Supplier shall not be entitled to any relief from its obligations under the KPIs or to any increase in the Price to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

5. PART B: BUSINESS CONTINUITY PLAN - PRINCIPLES AND CONTENTS

- 5.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes and operations facilitated by the Services remain supported and to ensure continuity of the business operations supported by the Services including, unless the Authority expressly states otherwise in writing:
 - (a) the alternative processes (including business processes), options and responsibilities that may be adopted in the event of a failure in or disruption to the Services; and
 - (b) the steps to be taken by the Supplier upon resumption of the Services in order to address any prevailing effect of the failure or disruption including a root cause analysis of the failure or disruption.
- 5.2 The Business Continuity Plan shall:
 - (a) address the various possible levels of failures of or disruptions to the Services;
 - (b) set out the services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Services (such services and steps being the "**Business Continuity Services**");
 - (c) specify any applicable KPI with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the KPI in respect of other Services during any period of invocation of the Business Continuity Plan; and
 - (d) clearly set out the conditions and/or circumstances under which the Business Continuity Plan is invoked.

6. PART C: DISASTER RECOVERY PLAN - PRINCIPLES AND CONTENTS

- 6.1 The Disaster Recovery Plan shall be designed so as to ensure that if a Disaster occurs the Supplier ensures continuity of the business operations of the Authority supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.
- 6.2 The Disaster Recovery Plan shall be invoked only if a Disaster occurs.
- 6.3 The Disaster Recovery Plan shall include:
 - (a) the technical design and build specification of the disaster recovery system;

- (b) details of the procedures and processes to be put in place by the Supplier and any Sub-Contractors in relation to the disaster recovery system and the provision of the disaster recovery services and any testing of the same including the following;
 - (i) data centre and disaster recovery site audits;
 - (ii) backup methodology and details of the Supplier's approach to data back-up and data verification;
 - (iii) identification of all potential Disaster scenarios;
 - (iv) risk analysis;
 - (v) documentation of processes and procedures;
 - (vi) hardware configuration details;
 - (vii) network planning including details of all relevant data networks and communication links;
 - (viii) invocation rules;
 - (ix) Service recovery procedures; and
 - (x) steps to be taken upon resumption of the Services to address any prevailing effect of the failure or disruption of the Services;
- (c) any applicable KPI with respect to the provision of the disaster recovery services and details of any agreed relaxation to the KPI in respect of other Services during any period of invocation of the Disaster Recovery Plan;
- (d) details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;
- (e) access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and
- (f) testing and management arrangements.

7. REVIEW AND AMENDMENT OF THE BCDR PLAN

- 7.1 The Supplier shall review part or all of the BCDR Plan (and the risk analysis on which it is based):
- (a) at least once every 6 Months;
 - (b) within 3 Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 9; and
 - (c) where the Authority requests any additional reviews (over and above those provided for above by notifying the Supplier to such effect in

writing, whereupon the Supplier shall conduct such reviews in accordance with the Authority's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Authority for Approval. The costs of both Parties of any such additional reviews shall be met by the Authority except that the Supplier shall not be entitled to charge the Authority for any costs that it may incur above any estimate without Approval.

7.2 Each review of the BCDR Plan pursuant to Paragraph 7.1 above shall be a review of the procedures and methodologies set out in the BCDR Plan and shall assess their suitability having regard to any change to the Services or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original Approval of the BCDR Plan or the last review of the BCDR Plan and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within the period required by the BCDR Plan or, if no such period is required, within such period as the Authority shall reasonably require. The Supplier shall, within 20 Working Days of the conclusion of each such review of the BCDR Plan, provide to the Authority a report setting out:

- (a) the findings of the review;
- (b) any changes in the risk profile associated with the Services; and
- (c) the Supplier's proposals for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan following the review detailing the impact (if any and to the extent that the Supplier can reasonably be expected to be aware of the same) that the implementation of such proposals may have on any services or systems provided by a third party (the "**Risk Profile Proposals**"),

being the "**BCDR Plan Review Report**".

7.3 Following receipt of the BCDR Plan Review Report and the Risk Profile Proposals, the Authority shall:

- (a) review and comment on the BCDR Plan Review Report and the Risk Profile Proposals as soon as reasonably practicable; and
- (b) notify the Supplier in writing that it approves or rejects the BCDR Plan Review Report and the Risk Profile Proposals no later than 20 Working Days after the date on which they are first delivered to the Authority.

7.4 If the Authority rejects the BCDR Plan Review Report and/or the Risk Profile Proposals:

- (a) the Authority shall inform the Supplier in writing of its reasons for its rejection; and
- (b) the Supplier shall then revise the BCDR Plan Review Report and/or the Risk Profile Proposals as the case may be (taking reasonable account of

the Authority's comments and carrying out any necessary actions in connection with the revision) and shall re-submit a revised BCDR Plan Review Report and/or revised Risk Profile Proposals to the Authority for Approval within 20 Working Days of the date of the Authority's notice of rejection. The provisions of Paragraph 7.3 and this Paragraph 6.4 shall apply again to any resubmitted BCDR Plan Review Report and Risk Profile Proposals, provided that either Party may refer any disputed matters for resolution in accordance with Clause I1 (Dispute Resolution) at any time.

- 7.5 The Supplier shall as soon as is reasonably practicable after receiving Approval of the Risk Profile Proposals (having regard to the significance of any risks highlighted in the BCDR Plan Review Report) effect any change in its practices or procedures necessary so as to give effect to the Risk Profile Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Services.

8. TESTING OF THE BCDR PLAN

- 8.1 The Supplier shall test the BCDR Plan on a date to be agreed in the first Contract Year and then thereafter each Contract Year on the anniversary of the Service Commencement Date. Subject to Paragraph 8.2 below, the Authority may require the Supplier to conduct additional tests of some or all aspects of the BCDR Plan at any time where the Authority considers it necessary, including where there has been any change to the Services or any underlying business processes, or on the occurrence of any event which may increase the likelihood of the need to implement the BCDR Plan.
- 8.2 If the Authority requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Authority's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Authority provided prior to starting such test, the Supplier shall provide an accurate written estimate of the total costs payable by the Authority for Approval save for when the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.
- 8.3 The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with the Authority and shall liaise with the Authority in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Authority in this regard. Each test shall be carried out under the supervision of the Authority or its nominee.
- 8.4 The Supplier shall ensure that any use by it or any Sub-Contractor of "live" data in such testing is Approved in advance by the Authority's Senior Information Risk Owner. Copies of live test data used in any such testing shall be (if so required by the Authority) destroyed or returned to the Authority on completion of the test.
- 8.5 The Supplier shall, within 20 Working Days of the conclusion of each test, provide to the Authority a report setting out;
- (a) the outcome of the test;

- (b) any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and
 - (c) the Supplier's proposals for remedying any such failures.
- 8.6 Following each test, the Supplier shall take all reasonable measures requested by the Authority, (including requests for the re-testing of the BCDR Plan) to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier at no additional cost to the Authority, by the date reasonably required by the Authority and set out in such notice.
- 8.7 For the avoidance of doubt, the carrying out of a test of the BCDR Plan (including a test of the BCDR Plan's procedures) shall not relieve the Supplier of any of its obligations under the Contract.
- 8.8 The Supplier shall also perform a test of the BCDR Plan in the event of any major reconfiguration of the Services or as otherwise reasonably requested by the Authority.

9. INVOCATION OF THE BCDR PLAN

- 9.1 The Supplier shall ensure that it is able to implement the BCDR Plan at any time in accordance with its terms.
- 9.2 In the event of a complete loss of Service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Authority promptly of such invocation) such that the provision of the Services is resumed within 24 hours of the loss of Services or Disaster occurring. In all other instances the Supplier shall only invoke or test the BCDR Plan with Approval.

SCHEDULE 8 – PERFORMANCE, MANAGEMENT INFORMATION (MI) AND REPORTING

1. DEFINITIONS

- 1.1 Unless the context otherwise requires the following terms shall have the meanings given to them below. Other capitalised terms shall have the meanings given to them in the Terms & Conditions or Schedules in which they first appear.

"Aged Debt" means cases where overdue debt on the Debt Book is more than two years old from the date of crystallised debt. A debt becomes crystallised either when i) a convicted / part convicted Outcome and Final Defence Costs are received by the Supplier and an ICO Case to enable final balancing of debt due; or ii) the date the CCO is issued; whichever date is the latter in combined ICO / CCO Cases.

"CCO Checks" means an assurance check on the accuracy of CCO means assessment against disposable Capital and Equity as per the Criminal Legal Aid Contribution Regulations 2014.

"Debt Book" means the account book that records Defendants' debts.

"Extended Business Hours" means 8am to 10pm, Sunday to Saturday.

"Gross Debt Secured" means all debt secured at Interim Charging Order stage in the reporting month.

"High Court Writ" means a formal order that allows High Court enforcement officers the power to access a Defendant's business premises and seize assets to sell and repay debts owed.

"INL" means Initial Notification Letter.

"Initial Notification Letter" means the initial letter sent to the Defendant that introduces them to the debt collector company and notifies them of the amount due, how to contact the debt collection company and how to pay.

"MTD" means Month to Date.

"Month to Date" means the period starting at the beginning of the current calendar month and ending at the current date.

"Net Secured Debt" means Gross Secured Debt minus revoked Charging Orders and paid in full Charging Orders.

"PCL" means Post-conviction Reminder of Liabilities.

"Post-conviction Reminder of Liabilities" means a letter reminding a convicted Defendant that they may still be liable for Capital Contributions which will be confirmed once Final Defence Costs have been received.

"QC Checks" mean quality control checks undertaking by the Supplier on their own processes.

"Recognised Income" means the post-conviction crystallised cash payments that have been remitted to the Authority and recorded as cash receipts for the Authority.

"Records" means as it is detailed in paragraph 6.1 (Maintenance and Retention of Records).

"RL" means Reminder Letter.

"Reminder Letter" means a letter reminding a Defendant that either 1) payment is due in 5 days or 2) payment is now 5 days overdue

"Secured Debt" means when an Interim Charging Order has been obtained to protect the monies owed by the Defendant to the Authority by placing a charge on property owned.

"Service Credit" means an amount payable to the Supplier in respect of KPI achievement above the target Performance Levels as further provided in paragraph 3 below.

"Service Debit" means a deduction from monies due to the Supplier where KPI achievement does not meet the target Performance Level as further provided in paragraph 3 below.

"Performance Level" means the levels against which the performance of a KPI is measured, and as applicable, covers the target level to be achieved, and what constitutes a moderate failure level and a critical failure level.

"Third Party Debt Order" means an order of the court that freezes money held by a person, organisation or institution such as a bank or building society account, which might otherwise be paid to the debtor against whom a creditor has a judgment. A third party debt order will prevent the debtor having access to the money until the court makes a decision about whether or not the money should be paid to the creditor.

"Third Party Funds" means money that the Supplier has remitted to the Authority but is not able to be declared by LAA in its accounts. The money does not belong to LAA for accounting purposes until there has been a part guilty/guilty verdict and final defence costs. So although the Supplier will have remitted the cash, LAA has not been able to recognise the income, or the cash on the balance sheet. Instead the Authority holds the cash in a segregated account and classifies it as Third Party Funds until either the income can be recognised, or the money is refunded.

"YTD" means Year to Date.

"Year to Date" means that period running from the start of the current calendar year up to the current date.

2. **KEY PERFORMANCE INDICATORS (KPIs)**

- 2.1 Annex 1 (KPIs) of this Schedule sets out the 26 KPIs and their Target Performance Levels which the Parties agree shall be used to measure the performance of the Services by the Supplier.
- 2.2 The Supplier shall monitor its performance against each KPI (except where it is stated that the Authority shall monitor the performance in the source box of Annex 1 to this Schedule) and shall provide the Authority with a report detailing the level of service achieved in accordance with paragraph 6.3. The Authority will monitor and provide a report detailing

the level of Service delivery achieved by the Supplier for each KPI, the source of such data being as set out against 'Source:' in the description of the relevant KPI in Annex 1 to this Schedule 8.

- 2.3 The Supplier shall implement all monitoring tools and processes necessary to measure and report on their performance against the KPIs. These reports will provide a sufficient level of detail to verify compliance with the KPIs.
- 2.4 Formal measurement of performance against KPIs will commence three months after the Service Commencement Date.
- 2.5 The 'date of receipt' for performance management and KPI purposes will be considered as day zero (this means, for example, if a letter is received from a Defendant on a Tuesday before 16:00, the Tuesday will count as day zero, the Wednesday will be day 1 and the Thursday is day 2 etc.). Any requests received after 16:00 on any given Working Day will be recorded as being received the next Working Day.
- 2.6 The target Performance Levels shall be reviewed in January each year (commencing from Year 2) using the previous 12 months performance data. Any Changes will be implemented via the CCN in Schedule 12 (Change Control Forms) and will take effect from April of each year. The process for setting target Performance Levels is set out in Annex 4 of this Schedule.

3. KPI SERVICE CREDITS AND DEBITS

- 3.1 The Supplier may receive a payment of up to 10% of Service Costs as a Service Credit for performance that exceed the target Performance Levels for KPIs 1-3. The Supplier cannot gain Service Credits for any other KPI.
- 3.2 Service Debits may become payable by the Supplier in relation to KPIs 1-7, 9-11, 13, 15-21 and 24 where the performance level achieved by the Supplier against any given KPI in a month fails to meet the target Performance Levels set out in Annex 1.
- 3.3 The Service Credits or Service Debits to be applied shall be calculated on the basis of the following formula:

Total Collections KPI % (KPIs 1-3) + Total Admin KPI % (KPIs 4-7, 9-11, 13, 15-21 and 24).
- 3.4 The Authority shall use the performance monitoring reports provided by the Supplier in accordance with Annex 2 (Minimum Reporting Requirements) alongside access to the Supplier system to verify the calculation and accuracy of the Service Credits or Service Debits applicable to each monthly reporting period.
- 3.5 Service Credits are an increase of the amount payable in respect of the Services and do not include VAT. The Supplier shall increase the value of the appropriate invoice to reflect any agreed Service Credit that are due.
- 3.6 Service Debits are a reduction of the amount payable in respect of the Services and do not include VAT. The Supplier shall set off the value of any agreed Service Debits against the appropriate invoice.

4. SERVICE LEVEL FAILURE

- 4.1 In the event that

- 4.1.1 the Supplier is likely to or fails to meet any target Performance Level;
- 4.1.2 there is a Critical Service Level failure for 3 consecutive months or any 3 months in a rolling 6 month period for KPIs 1-3;
- 4.1.3 there is a moderate failure for 4 consecutive months or any 4 months in a rolling 6 month period;
- 4.1.4 there is a critical failure for 2 consecutive months or any 3 months in a rolling 6 month period for KPIs 4-26;
- 4.1.5 there is a moderate failure for 3 consecutive months or any 4 months in a rolling 6 month period for KPIs 4-26,

the Supplier shall immediately notify the Authority in writing and the Authority in its absolute discretion and without limiting any other of its rights may:

- 4.1.6 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Authority and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;
- 4.1.7 instruct the Supplier to comply with the enhanced monitoring process as described and in accordance with clause F3 (Enhanced Monitoring);
- 4.1.8 instruct the Supplier to comply with the Rectification Plan process as described in clause F2 (Rectification Plan Process);
- 4.1.9 if a Service Level Failure has occurred, deduct the applicable Service Debit payable by the Supplier to the Authority in accordance with Annex 1; and/or
- 4.1.10 if a Critical Service Level Failure has occurred, exercise its rights in accordance with paragraph 5.1.2 (Rectification Plan Process) to claim compensation for a Critical Service Level Failure or under clause H2 (Termination on Default) to terminate for Material Breach.

4.2 The Supplier acknowledges that any Service Level Failure may entitle the Authority to the rights set out in this Schedule 8, clause F2 (Rectification Plan Process) and clause H2 (Termination on Default) including the right to apply any Service Debits and that any Service Debit is a price adjustment and not an estimate of the loss that may be suffered by the Authority as a result of the Supplier's failure to meet any target Performance Level.

4.3 A Service Debit shall be the Authority's exclusive financial remedy for a Service Level Failure except where the Service Level Failure:

- 4.3.1 has arisen due to a Prohibited Act or wilful Default by the Supplier;
- 4.3.2 results in the corruption or loss of any Authority Data;
- 4.3.3 results in the Authority being required to make compensation payment to one or more third parties; and/or
- 4.3.4 the Authority is otherwise entitled to or does terminate this Contract pursuant to clause H2 (Termination on Default).

- 4.4 A Service Debit shall be the Authority's exclusive financial remedy for a Critical Service Level Failure except where the Authority has a right to compensation under paragraph 5.1.2.

5. RECTIFICATION

- 5.1 For as long as a Critical Service Level Failure has occurred and the Supplier is in the process of implementing a Rectification Plan in relation to such Critical Service Level Failure then the Authority may (in its sole discretion) notify the Supplier that:
- 5.1.1 the Service Credits and Service Debits that would otherwise have accrued during the relevant Service period shall not accrue; and
- 5.1.2 the Authority shall be entitled to withhold and retain as compensation a sum equal to any charges which would otherwise have been due to the Supplier in respect of that Service period.
- 5.2 The operation of paragraph 5.1 shall be without prejudice to the right of the Authority to terminate this Contract and/or to claim damages from the Supplier for Material Breach.

6. MANAGEMENT INFORMATION (MI)

- 6.1 During the Contract Term and for a period of 6 years thereafter, the Supplier shall maintain and retain Open Book Data.
- 6.2 The Supplier shall provide the Authority with the Management Information and financial reporting information set out below in paragraph 6.3 at the frequency indicated therein, in an agreed format.
- 6.3 The below table sets out the reporting requirements:

MI Reporting Reference	Management Information Requirement	Frequency
MI01	Month to Date (MTD) collections (for all debt types) against targets. Cumulative value of Charging Order applications still in pipeline. MTD case level data for Secured Debt.	Weekly
MI02	MTD collections (for all debt types) against targets. Cumulative value of Charging Order applications still in pipeline. MTD case level data for Secured Debt. Analysis of MTD/YTD CCO and ICO volumes and values against MTD/YTD forecast CCO and ICO volumes and values.	Monthly
MI03a	Monthly invoices for Service Costs and Enforcement Costs.	Monthly
MI03b	MTD/YTD invoice summaries (monthly and year to date) in respect of invoices incurred or relating to this Contract and/or the Services, including summary volumes and values of each unit category and total net/gross amount of each invoice and dates submitted.	Monthly
MI04	Cumulative collection percentage recovery rate (cash plus Secured Debt) against Debt Book value. To include raw case data.	Monthly
MI05	Monthly collections performance MTD and YTD against	Monthly

MI Reporting Reference	Management Information Requirement	Frequency
	MTD and YTD target broken down into cash collections, net Secured Debt, Secured Debt fully paid and converted to cash, revoked Secured Debt and total collections cash/net Secured Debt. To include YTD case level data.	
MI06	Report of cash remitted on cumulative volumes and values of convicted/part convicted Aged Debt cases where overdue debt is more than two years old from date of crystallised debt. To include case level data.	Monthly
MI07a	Report of MTD case level list and summary report of K&E Checks completed within 20 Working Days of convicted or part convicted Outcome or FDC.	Monthly
MI07b	Report of MTD case level list of K&E Checks quality assured in report MI07a by the Supplier with summary of % quality pass rates.	Monthly
MI08a	Report of MTD case level list and summary report of CCOs issued within 5 Working Days of K&E Check.	Monthly
MI08b	Report of MTD case level list of issued CCOs in report MI08a quality assured by the Supplier with summary of % quality pass rates.	Monthly
MI09	Report of MTD/YTD refunds of contributions / payments at case level paid within 5 Working Days of Authority Approval.	Monthly
MI10	MTD report of post-conviction letters sent out within 5 Working Days of conviction or part conviction to remind Defendants of possible post-conviction liability.	Monthly
MI11	MTD report of Defendant reminders sent 5 Working Days prior to payment due date.	Monthly
MI12	MTD report of Defendant reminders sent 5 Working Days after payment due date.	Monthly
MI13	MTD report of post-conviction reminders sent 5 Working Days after conviction/part conviction Outcome date.	Monthly
MI14	MTD report of action on queries/instructions from Authority taken within 5 Working Days.	Monthly
MI15	MTD report of enquiry from Defendant taken within 5 Working Days.	Monthly
MI16	MTD Complaints' performance log at case level.	Monthly
MI17	MTD and YTD write offs log (using Excel tabs, one for each month), for cases submitted to the Authority for Approval.	Monthly
MI18	Summary analysis of MTD/YTD volumes and value of pre-conviction (Income Contribution Order (ICO) contributions at date of issue, and new ICO accounts set up that are: <ul style="list-style-type: none"> a) standard ICOs; b) Income Evidence Sanction (IES) ICOs; c) ICOs received after trial finished; d) Phase 5 case (as defined in Schedule 1); and/or e) ICO data showing ICOs rejected from data feed with reasons for rejection. 	Monthly

MI Reporting Reference	Management Information Requirement	Frequency
MI19	<p>MTD/YTD summary analysis of volumes or volume of all Capital and Equity files received of which:</p> <ul style="list-style-type: none"> a) volume cases retained due to K&E over [Redacted] already declared; b) volume cases retained for further checking because K&E declared is > [Redacted]; or c) volume of cases returned to Authority as rejected due to [Redacted] K&E declared. 	Monthly
MI20	MTD/YTD CCOs issued volume and value of initial CCO contributions.	Monthly
MI21	MTD/YTD appeals volumes and value of initial appeal contributions.	Monthly
MI22	MTD/YTD volumes Charging Order applications, Attachment of Earnings applications, High Court Writ applications, Third Party Debt Orders, other enforcement order applications.	Monthly
MI23	Debt Book breakdown outstanding final total liability/debt due by pre conviction; post-conviction; post Final Defence Costs; appeals; Secured Debt and minus write offs with opening balance and closing balance.	Monthly
MI24	Summary Debt Book breakdown of final closing outstanding debt balance (less write-offs) by case stages volume and value pre conviction, post-conviction, post FDC, appeals, Secured Debt, pre-conviction enforcement, post-conviction enforcement, post FDC enforcement, and in prison.	Monthly
MI25	Current volume and value of open cases in a payment arrangement against the total book value (less write offs) of gross collections outstanding/not yet converted to cash broken down into pre conviction, post-conviction, post FDCs, appeals and Secured Debt cases.	Monthly
MI26	Current list at case level showing all high value debtors with initial contribution value over [Redacted] and status / progress notes.	Monthly
MI27	In month payment volumes and values due by scheme/status (ICO due within 28 calendar days, CCO due within 28 calendar days, ICO arrangements, CCO arrangements, appeals, FDCs greater than crystallised ICOs due in 28 calendar days, FDCs greater than crystallised ICOs in arrangement).	Monthly
MI28	In month payment volumes and values paid by scheme/case status. (ICO due within calendar 28 calendar days, CCO due within calendar 28 days, ICO arrangements, CCO arrangements, appeals, FDCs greater than crystallised ICOs due in 28 calendar days, FDCs greater than crystallised ICOs in arrangement, defaulted/other payments).	Monthly
MI29	Cumulative Enforcement Costs volume and value of total debt outstanding, and primary debt outstanding by enforcement category (Attachment of Earnings, High Court Writs, Charging Orders, Third Party Debt Orders and	Monthly

MI Reporting Reference	Management Information Requirement	Frequency
	other).	
MI30	Cumulative Enforcement Costs – % of recovery rates. Volume and value of each enforcement category that results in successful / part payment on main primary debt and on Enforcement Costs.	Monthly
MI31	Exceptions/housekeeping report where Outcomes, Sentence Order Dates and FDCs are still not yet received on data feed after 6 or 9 months in order to trigger case queries with the Authority.	Monthly
MI32	Cumulative payee behaviour analysis of debt crystallised cases (post FDC) by fully paid, partially paid, not paid volumes and values.	Monthly
MI33	Cumulative analysis of volumes and values of debt crystallised post FDC cases created by offence type and volume/value that are fully paid by offence type.	Monthly
MI34	Summary dashboard of key performance and contract management oversight data for monthly MI and Contract meetings.	Monthly
MI35	MTD/YTD contribution / payment received data at case level and method of payment analysis.	Monthly
MI36	Quarter/YTD Supplier's own QC Checks on their KPI performance showing type of check category, pass and fail outcomes for each check category and pass % rates for each check category.	Quarterly
MI37	Quarter/YTD Complaints trend summary – volumes, numbers and % justified, partially justified, unjustified and reasons for Complaint.	Quarterly
MI38	Quarter/YTD FOIAs and DSARs and requests to delete incorrect data – case level tracking report showing type of data request, date the request was received by the Supplier, and date information sent to the Authority.	Quarterly
MI39	Cumulative summary report on cash remitted. The report should be cumulative from the Service Commencement Date, with each new month's data being appended to the report.	Monthly
MI40	Detailed (to individual debtor level) cumulative remittance report. The report should be cumulative from the Service Commencement Date, with each new month's data being appended to the report.	Monthly
MI41	Detailed (to individual level) report of Defendant funds remitted to the Supplier's bank but not remitted to the Authority.	Monthly
MI42	Report of all recognised debt, including debt fully repaid, on the final day of the month (i.e. debt that has been crystallised by a guilty verdict, and is not currently on appeal).	Monthly
MI43	Report of all debt.	Monthly
MI44	Report of all live and closed crystallised cases since the beginning of the scheme.	Monthly

MI Reporting Reference	Management Information Requirement	Frequency
MI45	Summary report of income from all schemes, showing the opening cumulative position on 1st April, the values recognised monthly, and the closing cumulative position..	Monthly
MI46	Reconciliation report between the summary remittance data provided in report MI39 and the detailed remittance data provided in report MI40.	Monthly
MI47	Reconciliation report between recognised debt as per report MI43, and recognised debt as per report MI44 i.e. for crystallised debt only.	Monthly
MI48	Reconciliation report between remitted cash and Recognised Income.	Monthly
MI49	Detailed (to individual debtor level) remittance report for that week.	Weekly
MI50	Telephony report showing MTD/YTD volumes of calls received and answered / not answered and volumes of outgoing calls made / answered by Defendant.	Monthly

- 6.4 The minimum required reporting fields for the reports listed above are contained within Annex 2 (Minimum Reporting Requirements).
- 6.5 The Authority reserves the right to visit Supplier sites to carry out verification audits in accordance with clause E8 (Audit).
- 6.6 The Supplier commits to achieving continuous improvement and to support this, it shall have a process in place for reviewing opportunities and efficiency innovations.
- 6.7 The Supplier must designate a named individual as responsible for the accuracy, completeness, and timeliness of all MI reporting.

7. MAINTENANCE AND RETENTION OF RECORDS

- 7.1 In addition to its obligations in E8 (Audit), the Supplier shall retain and maintain all the records (including superseded records) referred to in paragraph 6.3 (together “**Records**”):
- 7.1.1 in accordance with the requirements of Good Industry Practice;
 - 7.1.2 in chronological order;
 - 7.1.3 in a form that is capable of audit; and
 - 7.1.4 at its own expense.
- 7.2 Without prejudice to clause E8 (Audit), the Supplier shall make the Records available for inspection to the Authority on request, subject to the Authority giving reasonable notice.
- 7.3 The Supplier shall, during the Contract Term and for a period of at least six years (or such other period as may be indicated by the Authority) following the expiry or termination of this Contract, maintain or cause to be maintained complete and accurate documents and Records in relation to the provision of the Services including but not limited to all Records.
- 7.4 The Records to be kept by the Supplier are:

- 7.4.1 this Contract, its Schedules, and all amendments to such documents;
- 7.4.2 all other documents which this Contract expressly requires to be prepared;
- 7.4.3 records relating to the appointment and succession of the Supplier CM and each member of the Key Personnel;
- 7.4.4 all operation and maintenance manuals and standard letter templates prepared by the Supplier for the purpose of delivering and maintaining the provision of the Services;
- 7.4.5 all formal notices, reports or submissions made by the Supplier to the Authority in connection with the provision of the Services;
- 7.4.6 all certificates, licences, registrations, or warranties in each case obtained by the Supplier in relation to the provision of the Services;
- 7.4.7 documents prepared by the Supplier in support of claims for the Price;
- 7.4.8 documents submitted by the Supplier pursuant to the Change procedure set out in clause F6 (Change);
- 7.4.9 documents submitted by the Supplier pursuant to the Supplier or the Authority invoking the dispute resolution procedure set out in clause I1 (Dispute Resolution);
- 7.4.10 documents evidencing any change in ownership or any interest in any or all of the shares in the Supplier and/or any guarantor, where such change may cause a Change of Control, and including documents detailing the identity of the persons changing such ownership or interest;
- 7.4.11 invoices and records related to VAT sought to be recovered by the Supplier;
- 7.4.12 financial records, including audited and un-audited accounts of the Supplier and any guarantor;
- 7.4.13 records required to be retained by the Supplier by Law, including in relation to health and safety matters and all consents;
- 7.4.14 all documents relating to the insurances to be maintained under this Contract and any claims made in respect of them; and
- 7.4.15 all other records, notices or certificates required to be produced.

8. CONTRACT PERFORMANCE ASSURANCE

- 8.1 The onus will be on the Supplier to demonstrate to the Authority Contract Manager (Authority CM) that robust internal processes are in place and the Supplier must provide the Authority CM with a quarterly report in relation to internal assurance and risk management and must demonstrate that all call handling, Complaints, and correspondence are dealt with to a satisfactory standard. The Supplier must provide all necessary assistance at nil charge to the Authority in supporting this assurance activity.

9. FINANCIAL ASSURANCE

- 9.1 The Supplier must designate a named individual as responsible for the accuracy, completeness, and timeliness of financial reporting. That individual must review and sign off (including recording evidence of sign off) all monthly reconciliations. Reconciliation report variances must not exceed [Redacted] and must be investigated and resolved in a timely manner (within 3 months or less).
- 9.2 The Supplier is a service organisation within the meaning of "ISAE3402, Assurance reports on controls at a service organisation". As such, the Supplier will be expected to engage external auditors to provide an ISAE3402-compliant assurance report annually for any year or part year covered by the contract. This annual assurance report should cover the period 1 April-31 March, and a final report should be made available to the Authority and the Authority's auditors (NAO) by 30 June each year.
- 9.3 The Authority is required to comply with International Financial Reporting Standards (IFRS) as interpreted by HMT's Financial Reporting Manual (FReM). These requirements include the production of financial statements on a full accruals' basis. The Supplier will be the primary custodian of Authority's financial data in relation to CCMT and will need to store and report on this data in a way that facilitates the Authority's compliance with IFRS and the FReM.
- 9.4 The Supplier must have sufficiently robust money laundering detection and fraud awareness processes in place in compliance with relevant legislation including the Money Laundering Regulations 2007, Proceeds of Crime Act 2012 (as amended by the Crime and Courts Act 2013 and the Serious Crime Act 2015) and the Financial Services and Markets Act 2000.
- 9.5 The Authority also reserves the right to carry out assurance activity to ensure that all money paid to the Supplier is correctly remitted back to the Authority.
- 9.6 The NAO carry out audits of the Authority under their statutory powers – either directly themselves or through their appointment of auditors to conduct work on their behalf. These audits include assurance of contributory cases and non-contributory cases as well as the regularity of the Authority's financial accounts which are heavily dependent on the accuracy of actions taken by the Supplier on the Authority's behalf to collect and remit monies and maintain accurate records of contributory cases and liabilities. The outcome of such audits will be shared between all Parties.
- 9.7 The NAO will be particularly interested in the following areas of the scheme:
- 9.7.1 collection of Capital evidence and completeness of Capital asset disclosures;
 - 9.7.2 Defendants who default on payments;
 - 9.7.3 control of refunds;
 - 9.7.4 the collection and remittance of money.
- 9.8 Where the Contractor intends to accept payments by debit/credit card the Contractor must have either:
- 9.8.1 Been certified by a Qualified Security Assessor and Approved Scanning Vendor (as applicable) as being compliant with the Payment Card Industry Security Standard (PCI DSS) version 1.1; or

- 9.8.2 completed an internal self-assessment and will adhere at all times to the terms of the PCI DSS and will notify the LAA promptly in writing of any changes in the Contractor's certification.
- 9.9 The Contractor must validate compliance in the manner deemed appropriate by the card scheme industry on an annual basis and provide the LAA with written evidence of compliance annually.
- 9.10 The Contractor will be responsible for any costs incurred to attain and maintain compliance with PCI DSS.
- 9.11 The Contractor must meet all PCI DSS requirements, on a continuing basis, including but not limited to any subsequent versions of the PCI DSS.
- 9.12 The Contractor must be responsible for the security of all Cardholder Data in the Contractor's possession
- 9.13 The Contractor must notify the LAA and the card scheme industry immediately if it knows or suspects that there has been, or will be, a breach of the security of Cardholder Data or of the PCI DSS.
- 9.14 The Contractor must indemnify the LAA, its subsidiaries, affiliates, officers, employees and agents from and against all actions, demands, costs, losses, penalties, damages, liability, claims and expenses (including but not limited to reasonable legal fees) whatsoever incurred by it or them arising from the Contractor's non-compliance with, or breach of, the PCI DSS or breach of Cardholder Data security.
- 9.15 The Contractor must cease taking payments, by debit/credit card, on behalf of the LAA in the event that the Contractor becomes non-compliant with, or suffers a breach of, the PCI DSS or breach of Cardholder Data security.

Annex 1 – KPIs

Reference:	KPI 1
Description:	A measure of the Supplier's YTD achievement, of the requirement to collect cash against the projected YTD annual cash collections target.
Performance Level:	Critical failure a) less than 90% Moderate failure b) 90.00% - 98.99% Target c) 99.00% - 102% Exceeding d) 102.01% - 115% Exceeding Plus e) Over 115%
Service/Debits Credits:	Critical -6% Moderate -3% Exceeding 3% Exceeding plus 6%
Calculation:	$\frac{\text{Collections}^{a.YTD}}{\text{Collections}^{c.YTD}} \times 100$ Where: <u>Collections^{a.YTD}</u> is the YTD actual cash collections <u>Collections^{c.YTD}</u> is the projected YTD cash collection target
Source:	<u>Collections^{a.YTD}</u> is calculated using backing data at report 5, Annex 2 Schedule 8 <u>Collections^{c.YTD}</u> is calculated using backing data at report 5, Annex 2, Schedule 8
Conditions:	Cash collected whilst Secured Debt remains partially paid will be remitted and reported as cash.
Exceptions:	N/A

Reference:	KPI 2
Description:	A measure of the Supplier's YTD achievement, to secure gross debt against YTD projected gross debt secured.
Performance Level:	Critical failure a) less than 80% Moderate failure b) 80.00% - 91.99% Target c) 92.00% - 108% Exceeding d) 108.01% - 120% Exceeding Plus e) Over 120%
Service Debits/Credits:	Critical Failure -2 % Moderate Failure -1 % Exceeding 1 % Exceeding Plus 2%
Calculation:	$\frac{\text{Collections}^{ans.YTD}}{\text{Collections}^{pns.YTD}} \times 100$ <p>Where:</p> <p>$\text{Collections}^{ans.YTD}$ is the actual YTD Gross Debt Secured</p> <p>$\text{Collections}^{pns.YTD}$ is the projected YTD Gross Debt Secured target</p>
Source:	<p>$\text{Collections}^{ans.YTD}$ is calculated using backing data at report 5, Annex 2, Schedule 8</p> <p>$\text{Collections}^{pns.YTD}$ is calculated using backing data at report 5, Annex 2, Schedule 8</p>
Conditions:	<p>Gross Debt Secured is all debt secured at Interim Charging Order stage in the reporting month.</p> <p>Cash collected whilst Secured Debt remains partially paid will be remitted and reported as cash. The Secured Debt collected will continue to be shown for accounting purposes as the original full amount (unless revoked or reassessed) until it has been paid in full and then it will be reduced to [Redacted].</p>
Exceptions:	N/A

Reference:	KPI 3
Description:	A measure of the Supplier's YTD achievement on cash collections on all Aged Debt cases (more than two years from debt crystallisation date) against YTD projected collections on all Aged Debt cases.
Performance Level:	Critical failure a) less than 90% Moderate failure b) 90.01% - 97.99% Target c) 98.00% - 102% Exceeding d) 102.01% - 110% Exceeding Plus e) Over 110.01%
Service Debits/Credits:	Critical Failure -2 % Moderate Failure -1% Exceeding 1% Exceeding Plus 2%
Calculation:	$\frac{Collections^{age.YTD}}{Collections^{page.YTD}} \times 100$ Where: <i>Collections^{age.YTD}</i> is the actual YTD Aged Debt cash collected <i>Collections^{page.YTD}</i> is the projected YTD Aged Debt collections target
Source:	<i>Collections^{age}</i> is calculated using backing data at report 6, Annex 2, Schedule 8 <i>Collections^{page}</i> is calculated using backing data at report 6, Annex 2, Schedule 8
Conditions:	Aged Debt cases are those where overdue debt on the Debt Book is more than two years old from date of crystallised debt. A debt will be crystallised either when: a) a convicted/part convicted Outcome and Final Defence Costs are received by the Supplier on an ICO Case to enable final balancing of debt due; OR b) the date the CCO is issued; OR c) whichever date above is the later in combined ICO/CCO Cases.
Exceptions:	N/A

Reference:	KPI 4
Description:	A measure of the Supplier's achievement, of the requirement to complete K&E checks within 20 working days of receipt of part convicted or convicted outcome or FDC.
Performance Level:	Target: 98% Moderate Failure Threshold: 97.9% and below Critical Failure Threshold: 80% and below
Service Debits:	% Moderate Failure -1% Critical Failure -2%
Calculation:	$\frac{K\&E\ checks^{pass}}{K\&E\ checks^{total}} \times 100$ <p>Where:</p> <p>$K\&E\ Checks^{pass}$ is the number of K&E checks that have been completed in the reporting month within 20 Working Days of receipt of part convicted or convicted outcome or FDC</p> <p>$K\&E\ Checks^{total}$ is the total number of K&E Checks that ave been completed in the reporting month</p>
Source:	<p>$K\&E\ Checks^{pass}$ is calculated using the backing data contained at report 7a, Annex 2, Schedule 8</p> <p>$K\&E\ Checks^{total}$ is calculated using the backing data contained at report 7a, Annex 2, Schedule 8</p>
Conditions:	A Working Day is defined as per the Contract definitions. For the avoidance of doubt any convicted or part convicted outcomes or any FDC's received by the supplier after 16:00hrs on any Working Day is counted as having been received the following working day.
Exceptions:	<p>This Target only applies to required K&E checks as per Business Rules in Schedule 1 Appendix B.</p> <p>Exceptions may be agreed at the discretion of the Authority, where the supplier needs to make further enquiries with the Defendant or Authority to clarify the correct amount of K&E and these enquiries/dates are recorded on the Supplier collection system.</p>

Reference:	KPI 5
Description:	A measure of the Supplier's achievement, of the requirement to complete K&E checks that meet the required quality.
Performance Level:	Target: 98% Moderate Failure Threshold: 97.9% and below Critical Failure Threshold: 80% and below
Service Debits:	Moderate Failure -1% Critical Failure -2%
Calculation:	$\frac{K\&E_{quality\ pass}}{K\&E_{quality\ tot}}$ <p>Where:</p> <p>$K\&E_{quality\ pass}$ = The total number of K&E checks that meet quality standards completed within the reporting month</p> <p>$K\&E_{quality\ total}$ = The total number of K&E checks completed within the reporting month</p>
Source:	<p>$K\&E_{quality\ pass}$ is calculated using the backing data contained at report 7b, Annex 2 to this Schedule</p> <p>$K\&E_{quality\ total}$ is calculated using the backing data contained at report 7b Annex 2 to this Schedule.</p>
Conditions:	N/A
Exceptions:	This Target only applies to required K&E checks as per Business Rules in Schedule 1 Appendix B.

Reference:	KPI 6
Description:	A measure of the Supplier's achievement, of the requirement to issue CCO's within 5 working days of K&E checks or receipt of FDCs.
Performance Level:	Target: 98% Moderate Failure Threshold: 97.9% and below Critical Failure Threshold: 90% and below
Service Debits:	Moderate Failure -1% Critical Failure -2%
Calculation:	$\frac{CCO^{pass}}{CCO^{total}} \times 100$ <p>Where:</p> <p>CCO^{pass} the total number of CCOs that have been issued in the reporting month within 5 Working Days of K&E checks or receipt of FDCs</p> <p>CCO^{total} is the total amount of CCOs that have been issued in the reporting month</p>
Source:	<p>CCO^{pass} is calculated using the backing data contained at report 8a, Annex 2 to this Schedule</p> <p>CCO^{total} is calculated using the backing data contained at report 8a, Annex 2 to this Schedule</p>
Conditions:	A Working Day is defined as per the contract definitions. For the avoidance of doubt any K&E check completed after 16:00hrs or any FDC received by the supplier from the Authority after 16:00hrs on any Working Day is counted as having been received the following working day
Exceptions:	N/A

Reference:	KPI 7
Description	A measure of the Supplier's achievement, of the requirement to issue CCO's that pass the required quality check.
Performance Level	Target: 98% Moderate Failure Threshold: 97.9% and below Critical Failure Threshold: 90% and below
Service Debits:	Moderate Failure -1% Critical Failure -2%
Calculation:	$\frac{CCO^p}{CCO^t} \times 100$ <p>Where:</p> <p>CCO^p = The total number of CCO cases that have been issued that pass the required quality check in the reporting month</p> <p>CCO^t = The total number of CCO cases issued in the reporting month.</p>
Source:	<p>CCO^p is calculated using the data contained within report 8, Annex 2 to this Schedule</p> <p>CCO^t is calculated using the contained within report 8 Annex 2 to this Schedule</p>
Conditions:	N/A
Exceptions:	N/A

Reference:	KPI 8
Description	A measure of the Supplier's achievement, of the requirement to send weekly remittance reports within 1 Working Day following the weekend.
Performance Level	Target: 100% Moderate Failure: 75% and below Critical Failure Threshold: 50% and below
Service Debits:	N/A
Calculation:	$\frac{Collections^{remittance}}{Weeks} \times 100$ <p>Where $Collections^{remittance}$ is the number of remittance reports received within the 1 day measure for each full week of the reporting month.</p> <p>$weeks$ is the number of weeks in the reporting month where a report was available.</p>
Source:	Authority to complete weekly report log to confirm 100% receipt each week in the month
Conditions:	A Working Day is defined as per the contract definitions. The collection remittance week ends on a Sunday at 16:00hrs. Remittance reports must be sent to the Authority by 23:59 on the first Working Day following the weekend.
Exceptions:	Weekly remittance reports are not required for part weeks in the reporting month i.e., where month end is on a Mon, Tues, Wed or Thu – a separate weekly remittance report for those days is not needed for the remainder of that reporting month.

Reference:	KPI 9
Description	A measure of the Supplier's achievement, to pay Refunds to Defendants within 5 Working Days of approval by the Authority.
Performance Level	Target: 98% Moderate Failure: 97.9% and below Critical Failure Threshold: 90% and below
Service Debits	Moderate Failure -1% Critical Failure -2%
Calculation:	$\frac{Refund^P}{Refund^T} \times 100$ <p>Where:</p> <p>$Refund^P$ = The total number of Refunds issued by the Supplier within 5 Working Days following Authority approval in the reporting month</p> <p>$Refund^T$ = The total number of Refunds issued by the Supplier in the reporting month</p>
Source:	<p>$Refund^P$ = is calculated using the data contained within report 16 in Annex 2 of this Schedule</p> <p>$Refund^T$ = is calculated using the data contained within report 16 in Annex 2 of this Schedule</p>
Conditions:	A Working Day is defined as per the contract definitions. For the avoidance of doubt any approval received by the supplier from the Authority after 16:00hrs on any Working Day is counted as having been received the following working day
Exceptions:	N/A

Reference:	KPI 10
Description	A measure of the Supplier's achievement, to provide monthly and quarterly MI and financial reports in accordance with Annex 2 and 3 of this Schedule, within 7 Calendar Days following month and/or quarter end.
Performance Level	Target: 100% within 7 calendar days Critical Failure Threshold: Any report over 7 calendar days
Service Debits:	Critical Failure -1%
Calculation:	$Reports \frac{(r)}{d} \times 100$ <p>Reports (r) is the number of reports received within 7 calendar days following month and/or quarter end</p> <p>Reports (d) is the number of reports due within 7 calendar days following month and/or quarter end</p>
Source:	Authority to complete monthly log to confirm 100% receipt by day 7
Conditions:	A Calendar Day is defined as per the contract definitions.
Exceptions:	<p>An extension to 7 Calendar Days can be agreed in advance where the 7th Calendar Day falls:</p> <p>a) on a Saturday or Sunday; OR</p> <p>b) on a bank holiday (e.g. if the 7th calendar day is Good Friday the next Working Day would be the Tuesday following the Easter Monday).</p>

Reference:	KPI 11
Description	A measure of the Supplier's achievement, to provide accurate financial reports to the Authority in accordance with Annex 3 of this Schedule.
Performance Level	Target: 100% Critical Failure: Any financial report requiring correction
Service Debits:	Critical Failure -1%
Calculation:	$Error^{MI} = 0$ Where: $Error^{MI}$ is the error rate of specifications in Annex 3 of this Schedule
Source:	Authority (Finance Team) to complete monthly log to confirm 100% accuracy
Conditions:	A failure would be any financial error affecting the ability of the Authority to update their accounts correctly within that month
Exceptions:	Minor errors that are quickly rectified and do not affect the ability of the Authority to update their accounts correctly within that month

Reference:	KPI 12
Description	A measure of the Supplier's achievement, to provide accurate monthly and quarterly MI reports in accordance with Annex 2 of this Schedule.
Performance Level	Achieving Target: 100% accuracy Moderate Failure threshold – any MI report requiring correction
Service Debits:	N/A
Calculation:	$Error^{MI} = 0$ Where: $Error^{MI}$ is the error rate of specifications in Annex 2 of this Schedule
Source:	Authority (Contract Team) to complete monthly log to confirm 100% accuracy
Conditions:	A failure would be where the report affects the ability of the Authority to validate and score any KPI performance accurately in that month.
Exceptions:	Minor errors that are quickly rectified and do not affect the ability of the Authority to account for or review performance effectively

Reference:	KPI 13
Description	A measure of the Supplier's achievement, to reconcile variances in excess of [Redacted] within the financial reconciliation reports within 3 months of the submitted report.
Performance Level	Target: 100% of reports reconciled within 3 months of errors being identified Critical Failure – any reports that don't reconcile within 3 months of identification
Service Debits	Critical Failure -1%
Calculation:	$\text{Financial error}^{\geq \text{£100k}} = 0$ <p>Where:</p> $\text{Financial error}^{\geq \text{£100k}}$ <p>is the number of financial errors over [Redacted] remaining after 3 months</p>
Source:	Authority to complete monthly log to confirm 100% reconciliation of financial reports
Conditions:	<p>A failure would be where reconciliation reports do not reconcile and are not remediated within 3 months.</p> <p>Example. If a report ending 30 April is received by the Authority 7 May and a reconciliation issue is raised by the Authority to the Supplier on 11 May, then month 1 will start on 1 May and end on 31 July.</p>
Exceptions:	N/A

Reference:	KPI 14
Description:	A measure of the Supplier's achievement, to respond to ad hoc data requests within 7 Working Days of receipt from the Authority during the reporting month.
Performance Level:	Target: 100% within 7 Working Days Moderate Failure Threshold: Any ad hoc report received after 7 Working Days
Service Debits:	N/A
Calculation:	$\text{Requests} \frac{R}{Re} \times 100$ <p>Where R = the number of requests responded to within 7 Working Days from receipt</p> <p>Where Re = the total number of requests responded to during the reporting month</p>
Source:	Authority to complete monthly log to confirm 100% received within 7 working days
Conditions:	A Working Day is defined as per the contract definitions. For the avoidance of doubt any report received by the Authority from the Supplier after 16:00hrs on any Working Day is counted as having been received the following Working Day.
Exceptions:	An extension to the 7 Working Days can be agreed in advance with the Authority within 48 hours of the Supplier receiving the request from the Authority.

Reference:	KPI 15
Description:	A measure of the Supplier's achievement, to send an Initial Notification Letter (INL) within 2 Working Days of account set up for new CCMT ICO cases.
Performance Level:	Target: 95% Moderate Failure: 94.9% and below Critical Failure Threshold: 90% and below
Service Debits:	% Moderate Failure -0.5% Critical Failure -1%
Calculation:	$\frac{INL^S}{INL^T} \times 100$ <p>Where:</p> <p>INL^S = The total number of INLs sent within 2 Working Days of account set up in the reporting month</p> <p>INL^T = The total number of INLs sent in the reporting month</p>
Source:	<p>INL^S is calculated using the data contained within report 10 in Annex 2 of this Schedule.</p> <p>INL^T is calculated using the data contained within report 10 in Annex 2 of this Schedule.</p>
Conditions:	A Working Day is defined as per the contract definitions. For the avoidance of doubt any account set up after 16:00hrs on any Working Day is counted as having been set up the following working day
Exceptions:	N/A

Reference:	KPI 16
Description	A measure of the Supplier's achievement, to send a Post-conviction reminder of liabilities letter (PCL) within 5 Working Days following notification of conviction or part conviction outcome.
Performance Level	Target: 95% Moderate Failure: 94.9% and below Critical Failure Threshold: 90% and below
Service Debits:	Moderate Failure -0.5% Critical Failure -1%
Calculation:	$\frac{PCL^S}{PCL^T} \times 100$ <p>Where:</p> <p>PCL^S = The total number of PCLs sent within 5 Working Days following notification of conviction or part conviction outcome.</p> <p>PCL^T = The total number of PCLs sent in the reporting month following notification of conviction or part conviction outcome.</p>
Source:	<p>PCL^S is calculated using the data contained within report 11 in Annex 2 of this Schedule.</p> <p>PCL^T is calculated using the data contained within report 11 in Annex 2 of this Schedule.</p>
Conditions:	A Working Day is defined as per the contract definitions. For the avoidance of doubt notification of conviction or part conviction received by the Supplier after 16:00hrs on any Working Day is counted as having been received the following working day
Exceptions:	N/A

Reference:	KPI 17
Description	A measure of the Supplier's achievement, to send a reminder letter (RL) to defendants 5 Working Days prior to payment being due
Performance Level	Target: 95% Moderate Failure: 94.9% and below Critical Failure Threshold: 90% and below
Service Debits:	Moderate Failure - 0.5% Critical Failure -1%
Calculation:	$\frac{RL^S}{RL^T} \times 100$ <p>Where:</p> <p>RL^S = The total number of RLs sent within 5 Working Days prior to payment being due</p> <p>RL^T = The total number of RLs sent in the reporting month for cases where payment is due</p>
Source:	<p>RL^S is calculated using the data contained within report 12 in Annex 2 of this Schedule.</p> <p>RL^T is calculated using the data contained within report 12 in Annex 2 of this Schedule.</p>
Conditions:	A Working Day is defined as per the contract definitions.
Exceptions:	N/A

Reference:	KPI 18
Description:	A measure of the Supplier's achievement, to send a reminder letter (RLOD) to defendants 5 Working Days after a payment due date has been missed.
Performance Level	Target: 95% Moderate Failure: 94.9% and below Critical Failure Threshold: 90% and below
Service Debits:	Moderate Failure - 0.5% Critical Failure -1%
Calculation:	$\frac{RLOD^S}{RLOD^T} \times 100$ <p>Where:</p> <p>$RLOD^S$ = The total number of reminder letters sent within 5 Working Days following a missed payment date.</p> <p>$RLOD^T$ = The total number of reminder letters sent in the reporting month following missed payment dates.</p>
Source:	<p>$RLOD^S$ is calculated using the data contained within report 13 in Annex 2 of this Schedule.</p> <p>$RLOD^T$ is calculated using the data contained within report 13 in Annex 2 of this Schedule.</p>
Conditions:	A Working Day is defined as per the contract definitions.
Exceptions:	N/A

Reference:	KPI 19
Description:	A measure of the Supplier's achievement, to complete action on case updates or case queries from the Authority within 5 Working Days of receipt of the daily task sheets from the Authority.
Performance Level:	Target: 95% Moderate Failure: 94.9% and below Critical Failure Threshold: 90% and below
Service Debits:	Moderate Failure -0.5% Critical Failure -1%
Calculation:	$\frac{Queries^{pass}}{Queries^{total}} \times 100$ <p>Where:</p> <p>$Queries^{pass}$ is the number of queries the Supplier has reported as being actioned within 5 Working Days in the reporting month</p> <p>$Queries^{total}$ is the number of queries the Supplier has actioned in the reporting month</p>
Source:	<p>$Queries^{pass}$ is calculated using the backing data contained at report 14, Annex 2 of this Schedule</p> <p>$Queries^{total}$ is calculated using the backing data contained at report 14, Annex 2 of this Schedule</p>
Conditions:	A Working Day is defined as per the contract definitions. For the avoidance of doubt any case updates or case queries after 16:00hrs on any Working Day is counted as having been received the following working day
Exceptions:	N/A

Reference:	KPI 20
Description:	A measure of the Supplier's achievement, to resolve enquiries from Defendants within 5 Working Days of receipt of query contact.
Performance Level:	Target: 95% Moderate Failure: 94.9% and below Critical Failure Threshold: 90% and below
Service Debits:	Moderate Failure -0.5% Critical Failure -1%
Calculation:	$\frac{E^R}{E^T} \times 100$ <p>Where:</p> <p>E^R = The total number of enquiries from defendants resolved within 5 Working Days of receipt of query</p> <p>E^T = The total number of enquiries from defendants responded to in the reporting month</p>
Source:	<p>E^R is calculated using the data contained within report 15 in Annex 2 of this Schedule.</p> <p>E^T is calculated using the data contained within report 15 in Annex 2 of this Schedule.</p>
Conditions:	A Working Day is defined as per the contract definitions. For the avoidance of doubt any enquiry received from a defendant after 16:00hrs on any Working Day is counted as having been received the following working day
Exceptions:	N/A

Reference:	KPI 21
Description:	A measure of the Supplier's achievement to respond to complaints from Defendants within 10 Working Days from the date of the complaint being raised.
Performance Level:	Target: 95% Moderate Failure: 94.9% and below Critical Failure Threshold: 90% and below
Service Debits:	Moderate Failure -0.5% Critical Failure -1%
Calculation:	$\frac{C^R}{C^T} \times 100$ <p>Where:</p> <p>C^R = The total number of complaints replied to within the reporting month, within 10 Working Days from the date of the complaint being raised</p> <p>C^T = The total number of complaints replied to in the reporting month</p>
Source:	<p>C^R is calculated using the data contained within report 16 in Annex 2 of this Schedule.</p> <p>C^T is calculated using the data contained within report 16 in Annex 2 of this Schedule.</p>
Conditions:	A Working Day is defined as per the contract definitions. For the avoidance of doubt any complaint received by the supplier after 16:00hrs on any Working Day is counted as having been received the following working day
Exceptions:	N/A

Reference:	KPI 22
Description:	A measure of the Supplier's achievement, to refer write offs to the Authority within 6 months of all evidence being made available.
Performance Level:	Target: 95% Moderate Failure: 94.9% and below Critical Failure Threshold: 90% and below
Service Debits:	N/A
Calculation:	$\frac{Write\ Off^{Pass}}{Write\ Off^{Total}} \times 100$ <p>Where:</p> <p>$Write\ Off^{Pass}$ is the number of write offs referred in the reporting month by the Supplier which have been referred within 6 months of all evidence being made available to Supplier.</p> <p>$Write\ Off^{Total}$ is the total number of write offs referred for approval in the reporting month by the Supplier to the Authority.</p>
Source:	<p>$Write\ Off^{Pass}$ is calculated using the backing data contained at report 17, Annex 2 to this Schedule 8.</p> <p>$Write\ Off^{Total}$ is calculated using the backing data contained at report 17, Annex 2 to this Schedule 8.</p>
Conditions:	The 6 months starts when the Supplier has received the final piece of evidence to support write off
Exceptions:	N/A

Reference:	KPI 23
Description:	A measure of the Supplier's achievement, to provide read only access to the Supplier Collection System to licensed caseworkers at the Authority during Extended Business Hours.
Performance Level:	Target: 98% Moderate Failure: 97.9% and below Critical Failure Threshold: 90% and below
Service Debits:	N/A
Calculation:	The total number of hours the collection system was available to Authority licensed Caseworkers during the reporting month /The total number of available Authority Business Hours within the reporting month
Source:	Authority to keep log of reported incidents/downtime
Conditions:	LAA Business Hours are defined as From 6am to 10pm Monday to Saturday for the purposes of this KPI
Exceptions:	Planned outages such as maintenance work or IT/Software updates agreed in advance with the Authority.

Reference:	KPI 24
Description:	A measure of the Supplier's achievement, to upload data feed information from the Authority to their Collection system within 5 working days of data feed being sent.
Performance Level:	Target: 95% Moderate Failure: 94.9% and below Critical Failure Threshold: 90% and below
Service Debits:	Moderate Failure -0.5% Critical Failure -1%
Calculation:	$\frac{Data\ Feed^{pass}}{Data\ Feed^{Total}} \times 100$ <p>Where:</p> <p>$Data\ Feed^{pass}$ is the number of data feed outputs from the Authority's random sample that were uploaded in the reporting month to the Collection System, within 5 Working Days</p> <p>$Data\ Feed^{Total}$ is the total number of data feed outputs uploaded by the Supplier from the Authority's random sample of the data feed for the reporting month.</p>
Source:	Log of data feed transmissions randomly sampled by the Authority for the month with pass rates.
Conditions:	N/A
Exceptions:	Any data feed uploads relating to New ICO accounts which must be uploaded and set up on the Supplier's collection system within 1 working day.

Reference:	KPI 25
Description:	A measure of the Supplier's achievement, to provide defendants with 24/7 access (excluding planned outages) to an online payment system.
Performance Level:	Target: 98% Moderate Failure: 97.9% and below Critical Failure Threshold: 90% and below
Service Debits:	N/A
Calculation:	Hours system available to defendants (net of planned outage/maintenance) / Hours within the reporting month
Source:	Authority to keep log of reported incidents/downtime
Conditions:	N/A
Exceptions:	Planned outages such as maintenance work or IT/Software updates agreed in advance with the Authority.

Reference:	KPI 26
Description:	Percentage of all companies in the supply chain under the Contract to have implemented measures to improve the physical and mental health and wellbeing of Staff;
Performance Level:	Target: 100% Moderate Failure: 99.9% - 90% Critical Failure Threshold: 89.9% and below
Service Debits:	N/A
Calculation:	Supplier policies/procedures which include measures implemented to improve the physical and mental health and wellbeing of staff.
Source:	Supplier to provide the Authority with policies/procedures.
Conditions:	N/A
Exceptions:	N/A

Annex 2 – Minimum Reporting Requirements

The tables in this Annex 2 set out the compulsory requirements that each report must contain.

1. **Weekly reports.** In order to fulfil its financial reporting requirements, the Authority will require the following core reports from the Supplier weekly by 12 noon on first Working Day following week end:

Report 1 - Weekly Management Information	<ul style="list-style-type: none"> • MTD cash collections actuals against target. • MTD net Secured Debt actuals against target (i.e. gross Secured Debt minus paid and revoked Secured Debt). • MTD collection totals (cash plus net Secured Debt) actuals against target. • Cumulative number / value of Charging Order applications still outstanding in the pipeline with the date the Interim Charging Order is expected back from Court. <p>To be backed up with MTD case level data for Secured Debt showing:</p> <ul style="list-style-type: none"> • Authority MAAT reference; • Supplier unique ID; • surname.
--	---

2. **Interim monthly report.** In order to fulfil management reporting requirements, the Authority will require the following reports from the Supplier by 12 noon on first Working Day following month end:

Report 2 - Monthly interim Management Information	<ul style="list-style-type: none"> • MTD cash collections actuals against target; • MTD net Secured Debt actuals against target (i.e. gross Secured Debt minus paid in full and revoked Secured Debt); • MTD cash collections of aged debt actuals against target • MTD total cash collections (cash, aged debt cash plus net Secured Debt) actuals against target; • number /value of Charging Order applications still outstanding in the pipeline with the date the Interim Charging Order is expected back from Court; • narrative to explain MTD variations against MTD forecast; • Analysis of MTD/TD CCO volumes and ICO volumes against MTD/YTD forecast CCO volumes and ICO volumes; • Analysis of MTD/YTD CCO values and ICO values against MTD /YTD forecast CCO values and ICO values. <p>To be backed up with MTD case level data showing</p> <ul style="list-style-type: none"> • Authority MAAT reference • Supplier unique ID • surname; • collections received by scheme in that month and date received broken down by CCMT pre conviction scheme, K&E post-conviction scheme and appeals; • cumulative breakdown of secured debt by stages – Interim Charging Order; Final Charging Order; paid in full; revoked; and varied.
---	--

3. **Monthly reports.** In order to fulfil contract management oversight and KPI performance reporting requirements, the Authority will require the following reports from the Supplier by 23:59 hours 7 calendar days following month end or quarter end:
 - 3.1 KPIs will be monitored and assessed internally by the Supplier on a monthly basis and a self-assessment score sent to the Authority CM with supporting reporting evidence as below. The Authority CM would then assess and validate the monthly score provided by the Supplier.
 - 3.2 For monthly Contract meetings a dashboard with a layout to be agreed with Authority CM is required summarising all key performance and Contract Management Information.

a. KPI Monthly performance reports to be provided by the Supplier

Report Number and title	Description
Report 3a - MTD Invoices	Monthly Invoices for 3a. Service and 3b. Enforcement
Report 3b - MTD/YTD invoices volumes and values summary	<p>Invoice summaries (MTD and YTD) in respect of invoices incurred or relating to Services provided and Enforcement Costs incurred to include:</p> <ul style="list-style-type: none"> • MTD/YTD gross and net amount total of each invoice broken down by service and enforcement and overall totals; • MTD/YTD summary volume and gross / net value breakdown of each unit price category on each invoice; • date submitted.
Report 4 - Cumulative collection % recovery rate	<p>Report of cumulative collection % recovery rate (cash plus Secured Debt) against Debt Book value of due/overdue collections (less write offs) by month initial case loaded, broken down by pre-conviction, post-conviction, post FDC, and appeals;</p> <p>To be backed up with raw case data showing:</p> <ul style="list-style-type: none"> • Authority MAAT reference; • Supplier unique ID; • case stage (pre conviction, post-conviction, post FDC, appeal); • debt due/overdue; • debt amount paid in cash and date remitted; • debt secured until paid in full.
<p>Report 5 - MTD/YTD cash and Secured Debt (gross and net) collections</p> <p>KPI 1 & 2</p>	<p>Report of monthly collections performance MTD and YTD report against MTD and YTD target, broken down into:</p> <ul style="list-style-type: none"> • cash collections; • net secured debt; secured debt fully paid and converted to cash; • revoked Secured Debt; • total collections cash/net Secured Debt. <p>To be backed up with YTD case level data showing:</p> <ul style="list-style-type: none"> • Authority MAAT reference; • Supplier unique ID; • surname; • cumulative breakdown of secured debt by stages – Interim Charging Order; Final Charging Order; paid in full; revoked; and varied.

<p>Report 6 - MTD/YTD Aged Debt conversion to cash report</p> <p>KPI 3</p>	<ul style="list-style-type: none"> Report of cash remitted on cumulative Values of convicted/part convicted Aged Debt cases where overdue debt is more than two years old from date of crystallised debt. <p>Date of crystallised debt is whichever is the later date:</p> <ul style="list-style-type: none"> Convicted/part convicted Outcome AND Final Defence Cost received on Income Contribution Order and final balance calculated; OR Date Capital Contribution Order issued. <p>Values to be backed up at case level data showing:</p> <ul style="list-style-type: none"> Authority MAAT reference; Supplier unique ID; surname; date of debt crystallisation or date CCO issued; type of case i.e. convicted ICO, CCO; combined ICO/CCO; cash remitted since crystallisation date; date cash remitted.
<p>Report 7a - MTD K&E Checks timeliness report of K&E Checks completed within 20 Working Days</p> <p>KPI 4</p>	<p>Report of MTD case level list and summary report of K&E Checks completed within 20 Working Days of convicted or part convicted Outcome or FDC to include:</p> <ul style="list-style-type: none"> ICO or K&E /CCO scheme; Authority MAAT reference; Supplier unique ID; K&E Checks completed that are chargeable to Authority as per Business Rules 3 and 4 in Appendix B of Schedule 1; date of convicted/part convicted Outcome on data feed (Rule 3 check); date of FDC (Rule 4 check); date K&E Checks completed; Outcome of check and whether found (over [Redacted]) or not found; pass/fail rate within KPI timescales; summary analysis of pass/fail % rate.
<p>Report 7b - MTD quality of K&E Checks</p> <p>KPI 5</p>	<p>Report of MTD case level list of K&E Checks quality assured from Report 7A by the Supplier with summary of % quality pass rates.</p> <ul style="list-style-type: none"> ICO or K&E /CCO scheme; Authority MAAT reference; Supplier unique ID; K&E Checks completed that are chargeable to Authority as per Business Rules 3 and 4 in Appendix B of Schedule 1; Outcome and whether K&E found (over [Redacted]) or not found; Outcome of quality pass/fail rate on case selected for QC check, MTD summary analysis of pass/fail % rate.
<p>Report 8a - MTD CCOs issued within 5 Working Days</p>	<p>Report of MTD case level list and summary report of CCOs issued within 5 Working Days K&E Check to include:</p> <ul style="list-style-type: none"> Authority MAAT reference; Supplier unique ID; date of K&E Check completed;

KPI 6	<ul style="list-style-type: none"> • date of Final Defence Cost on data feed; • date initial CCO issued; • pass/fail rate within KPI timescales; • summary analysis of pass/fail % rate.
Report 8b - MTD quality of CCOs issued KPI 7	Report of MTD case level list of issued CCOs from Report 8A quality assured by the Supplier with summary of % quality pass rates. <ul style="list-style-type: none"> • Authority MAAT reference; • Supplier unique ID; • date initial CCO issued; • pass/fail quality outcome of CCO selected for quality check • MTD summary analysis of pass/fail % rate.
Report 9 - MTD refunds of contributions within 5 Working Days after Authority Approval KPI 9	Report of MTD/YTD refunds of contributions / payments at case level paid within 5 Working Days of Authority Approval to include: <ul style="list-style-type: none"> • Authority MAAT reference; • Supplier Collection System unique ID; • surname of Defendant; • date returned from Authority with Approval; • refund amount of primary debt; • refund amount of 2% interest; • date refund issued by Supplier with letter; • refund method; • Supplier receipt number for refund; • debt type monies refunded e.g., income, interest.
Report 10 - MTD Initial Notification Letters within 2 Working Days of account set up KPI 15	MTD report of Initial Notification Letters set up within 2 Working Days of initial account set up for CCMT (ICO) cases to include: <ul style="list-style-type: none"> • Authority MAAT reference number; • Supplier Collection System unique ID; • surname of Defendant; • date of account set up for new ICO; • date Initial Notification Letter sent out; • pass <2 days or fail >2 days; • summary of pass rate for that month against total number of accounts set up for new ICOs.
Report 11 - MTD post-conviction liability reminders within 5 Working Days of conviction/part conviction KPI 16	MTD report of post-conviction letters sent out within 5 Working Days of conviction or part conviction to remind Defendants of possible post-conviction liability to include: <ul style="list-style-type: none"> • Authority MAAT reference number; • Supplier Collection System unique ID; • surname of Defendant; • date of Outcome (conviction or part-conviction); • date post-conviction letter sent out; • pass <5 days or fail >5 days; • summary of pass rate for that month against total number of post-conviction letters issued.
Report 12 - MTD reminders of debt due within 5 days	MTD Report of Defendant reminders sent 5 Working Days prior to payment due date to include: <ul style="list-style-type: none"> • Authority MAAT reference number;

of payment due date KPI 17	<ul style="list-style-type: none"> • Supplier Collection System unique ID; • surname of Defendant; • payment due date minus 5 days; • date reminder letter sent out; • pass <5 days or fail >5 days; • summary of pass rate for that month against total number of reminders issued.
Report 13 - MTD reminders of debt overdue within 5 days of payment overdue date KPI 18	MTD report of Defendant reminders sent 5 Working Days after payment due date to include: <ul style="list-style-type: none"> • Authority MAAT reference number; • Supplier Collection System unique ID; • surname of Defendant; • payment due date + 5 days; • date reminder letter sent out; • pass <5 days or fail >5 days; • summary of pass rate for that month against total number of reminders issued.
Report 14 - MTD action completed on queries from Authority within 5 Working Days KPI 19	MTD Report of action on queries/instructions from Authority taken within 5 Working Days to include: <ul style="list-style-type: none"> • Authority MAAT reference number; • Supplier Collection System unique ID; • surname of Defendant; • date query/instruction received from Authority on daily query log; • date action taken; • pass <5 days or fail >5 days; • summary of pass rate for that month against total number of Authority instructions/queries.
Report 15 - MTD action completed on enquiries from Defendant within 5 Working Days KPI 20	MTD Report of enquiry from Defendant taken within 5 Working Days to include: <ul style="list-style-type: none"> • Authority MAAT reference number; • Supplier Collection System unique ID; • surname of Defendant; • date of query from Defendant; • date of reply • pass <5 days or fail >5 days; • summary of pass rate for that month against total number of Defendant enquiries.
Report 16 - MTD Complaints from Defendant responded within 10 Working Days of receipt of Complaint KPI 21	MTD Complaints' performance log at case level to include: <ul style="list-style-type: none"> • Authority MAAT reference number; • Supplier Collection System unique ID; • surname; • date Complaint received; • date of response • pass <10 days or fail >10 days; • reason for Complaint; • justified, partially justified or unjustified.

<p>Report 17 - Log of all write offs at case level including date of referral to Authority, date of evidence and reason for write off</p> <p>KPI 22</p>	<p>MTD and YTD write offs log - (using Excel tabs, one for each month), for cases submitted to the Authority for Approval. Case level details to include:</p> <ul style="list-style-type: none"> • Authority MAAT reference number; • Supplier Collection System unique ID; • ICO or KE/CCO scheme • surname of Defendant; • date write off sent to Authority for Approval; • write-off amount primary debt; • write off amount Enforcement Costs; • write off amount total; • type – write-off reason/dropdown list (deceased; bankrupt; IVA; DRO; untraceable; uneconomic to pursue; outside jurisdiction; statute barred; lost charge due to admin error; repossession; negative Equity; unenforceable); • supporting notes to show location of dated evidence on Supplier Collection System; • YTD historical summary case list and summary analysis of all approved cases written off with MAAT ref number, reason for write off, value of total write off and date of closure of liability.
--	--

b. Monthly contract management reports to be provided by the Supplier for oversight purposes

<p>Report 18 - ICO pipeline</p> <p>MTD and YTD ICO volumes and values report</p>	<p>Summary analysis of MTD and YTD to include:</p> <ul style="list-style-type: none"> • volumes and value of pre-conviction ICOs at date of issue. New ICO accounts set up that are a) standard ICOs; b) Income Evidence Sanction (IES) ICOs; c) ICOs received after trial finished; and d) Phase 5 case; • ICO data showing ICOs rejected from data feed with reasons for rejection. • ICO volumes 1.paid in full, 2.withdrawn, 3.acquitted 4. liability reduced to [Redacted]] <p>All data above to be supported with case level data showing:</p> <ul style="list-style-type: none"> • Authority MAAT reference number; • Supplier Collection System unique ID; • surname of Defendant; • date of account set up, • date of rejection; • date of issue of initial ICO; • value of initial ICO; • Date when paid in full, withdrawn, acquitted or liability reduced to [Redacted] • summary analysis of YTD total issued, paid in full, withdrawn, acquitted , reduced to [Redacted] and average ICO value at issue.
<p>Report 19 - MTD/YTD K&E files pipeline</p>	<p>MTD/YTD summary analysis of volumes to include:</p> <ul style="list-style-type: none"> • volume of all Capital and Equity files received; of which: <ul style="list-style-type: none"> ○ volume cases retained due to K&E over [Redacted] declared sufficient to cover case cap;

	<ul style="list-style-type: none"> ○ volume cases retained for further checking because K&E declared is > [Redacted]; ○ volume cases returned to Authority as rejected due to [Redacted] or less K&E declared. <p>All data above to be supported with case level data showing:</p> <ul style="list-style-type: none"> • Authority MAAT reference number; • Supplier Collection System unique ID; • surname of Defendant; • date file retained by Supplier for K&E Checking because K&E > [Redacted] declared; • date file retained by Supplier because K&E > [Redacted] declared; • date of rejection due to [Redacted] or less K&E declared; • summary of YTD totals of each category above.
Report 20 – MTD and YTD CCO volumes and values	<p>MTD and YTD CCOs issued volume and value of initial CCO contributions.</p> <p>All data above to be supported with case level data showing:</p> <ul style="list-style-type: none"> • Authority MAAT reference number; • Supplier Collection System unique ID; • surname of Defendant; • date initial CCO issued; • value of initial CCO; • Date CCO paid in full or Revoked • summary analysis of YTD total issued, paid in full, revoked and average CCO value at issue.
Report 21 – MTD and YTD appeals volumes and values	<p>MTD and YTD appeals volumes and value of initial appeal contributions and paid in full .</p> <p>All data above to be supported with case level data showing:</p> <ul style="list-style-type: none"> • Authority MAAT reference number; • Supplier Collection System unique ID; • surname of Defendant; • date appeals contribution issued and paid in full. • Summary YTD analysis of appeals contributions issued and paid in full.
Report 22 - MTD/YTD enforcement volumes	<p>MTD and YTD volumes Charging Order applications, Attachment of Earnings applications, High Court Writ applications, Third Party Debt Orders, other enforcement order applications.</p> <p>All data above to be supported with case level data showing: -</p> <ul style="list-style-type: none"> • Authority MAAT reference number; • Supplier Collection System unique ID • ICO or KE/CCO scheme • surname of Defendant; • date of Court order application issued by enforcement type. • Volume and value of Charge orders at Interim stage • Summary YTD analysis of Charge Orders issued and at interim stage

Report 23a - Cumulative Debt Book breakdown	Outstanding final total liability/debt due by pre conviction; post-conviction; post Final Defence Costs; appeals; secured debt and minus write offs with opening balance and closing balance.
Report 23b - Cumulative Debt Book breakdown where debt over 31 days old	Summary outstanding final total liability/debt due over 31 days old by pre conviction; post-conviction; post FDCs; appeals; secured debt and minus write offs with opening balance and closing balance.
Report 24 - Cumulative Debt Book breakdown by case stage	Summary breakdown of final closing outstanding debt balance (less write-offs) by case stages volume and value – pre conviction, post-conviction, post FDC, appeals, Secured Debt, pre-conviction enforcement, post-conviction enforcement, post FDCs enforcement, and in prison.
Report 25 - Cumulative cases in current payment arrangement	<p>Current volume and value of cases in a payment arrangement against the total book value (less write offs) of gross collections outstanding/not yet converted to cash broken down into pre conviction, post-conviction, post FDCs, appeals and Secured Debt cases.</p> <p>To include:</p> <ul style="list-style-type: none"> • Authority MAAT reference number; • Supplier Collection System unique ID; • surname of Defendant; • case stage – pre conviction, post-conviction, post FDC, appeals, secured debt; • value of agreed payment arrangement due in that month.
Report 26 - Cumulative high value debtors with initial contribution >[Redacted] and progress indicators	<p>Current list at case level showing all high value debtors with initial contribution value over [Redacted] and status/ progress notes.</p> <p>Current list of debtors over [Redacted] to include:</p> <ul style="list-style-type: none"> • Authority MAAT reference number; • Supplier Collection System unique ID; • surname of Defendant; • amount of initial contribution over [Redacted]; • current reassessed amount of contribution where appropriate; • amount paid to date; • progress notes/open/closed status.
Report 27 - In month payments due	In month payments volumes and values due by scheme/status (ICO due within 28 calendar days, CCO due within 28 calendar days, ICO arrangements, CCO arrangements, appeals, FDCs greater than crystallised ICOs due in 28 calendar days, FDCs greater than crystallised ICOs in arrangement).
Report 28 - In month payments received	On month payments volumes and values paid by scheme/case status. (ICO due within 28 calendar days, CCO due within 28 calendar days, ICO arrangements, CCO arrangements, appeals, FDCs greater than crystallised ICOs due in 28 calendar days, FDCs greater than crystallised ICOs in arrangement, defaulted/other payments).
Report 29 - Enforcement Costs due	Cumulative Enforcement Costs volume and value of total debt outstanding, and primary debt outstanding by enforcement category (Attachment of Earnings, High Court Writs, Charging Orders, Third Party Debt Orders and other).
Report 30 - Enforcement Costs recovery rates	Cumulative Enforcement Costs – % of recovery rates. Volume and value of each enforcement category that results in successful / part payment on main primary debt and on Enforcement Costs.
Report 31 - Housekeeping	Exceptions/housekeeping report for cases where:

report/exceptions report	Ex1	CCMT – (Sentence Order Date) SOD received on date feed = Yes – Outcome received = No
	Ex2	CCMT – Outcome received on data feed =Yes - SOD=NO
	Ex3	CCMT - date account set up >6m - SOD=No OR Outcome=No
	Ex4	CCMT – SOD received on data feed date >9m - FDC=No
	Ex5	K&E – SOD received on data feed date >9m - FDC=No
	Ex6	K&E - sufficient KE SOD received date >9m - FDC=No
	Ex7	K&E - sufficient KE - No SOD - created date>9m - FDC=No
Report 32 - Payee behaviour and FDC analysis	Cumulative payee behaviour analysis of debt crystallised cases (post FDCs) by % of all debts fully paid, partially paid, not paid volumes and values. Cumulative average value of FDC in fully paid, partially paid, not paid and overall	
Report 33 - Payee behaviour by offence category	Cumulative analysis of volumes and values of debt crystallised post FDC cases created by offence type and volume/value that are fully paid by offence type.	
Report 34 - Dashboard	Summary dashboard of key performance and contract management oversight data for monthly MI and Contract meetings – contents and timing to be agreed with the Authority and no less than 2 days before MI meeting.	
Report 35 - Contribution/payment received data and method of payment analysis	MTD/YTD contribution / payment received data at case level including: <ul style="list-style-type: none"> • payment amount; • date payment received by Supplier; • method of payment to Supplier; i.e. direct debit, standing order, cheque, credit/debit card, online payment etc.; • Supplier receipt number; • debt type monies received against e.g., income, Capital, Equity. 	
Report 50 Telephony report	Telephony report showing MTD and YTD volumes of calls received and answered / not answered and volumes of outgoing calls made / answered by Defendant	

4. **Quarterly report.** In order to fulfil contract management oversight, the Authority will require the following reports from the Supplier by 23:59 hours 7 calendar days following quarter end. All reports to include case level data Authority MAAT reference and surname.

Report 36 - Supplier QC Checks	Quarter/YTD Supplier's own QC Checks on their KPI performance showing type of check category, pass and fail outcomes for each check category and pass % rates for each check category.
Report 37 - Supplier Complaints QC analysis	Quarter/YTD Complaints trend summary – volumes, numbers and % justified, partially justified, unjustified and reasons for Complaint.
Report 38 - Supplier volume of FOIAs and DSARs	Quarter/YTD FOIAs and DSARs and requests to delete incorrect data – case level tracking report showing type of data request, date the request received by the Supplier, and date information sent to the Authority.

Intentionally blank.

Annex 3 – Financial Reporting Guidance and Requirements

PART I

1. Financial reporting standards

The below table is provided for information only and sets out the accounting treatment for debt and income as cases go through the CCMT process.

Stage	Description	Accounting Treatment in Authority Financial Statements
Contribution notice/order issued	The level of contributions is determined and may subsequently be adjusted following Hardship Reviews etc. Defendants are required to start making contributions either by agreed monthly instalments or upfront payments. The Defendant's accounts may be in debit or credit, depending on payments made. The Supplier will collect and remit the cash to the Authority on a weekly basis.	Cash received is held as third party funds, as the Authority's entitlement to the funds is not yet settled. The contributions-owed debit or credit value is not recorded. No income is recognised.
Case verdict – not guilty	Contributions received are refunded to the Defendants (plus any interest accrued on the contributions) and any unpaid contributions-owed balance is reversed out. The Supplier will process the refunds and net them off the weekly remittance of cash received.	The refund payments are disclosed as gross outflows of third party funds.
Case verdict – guilty – Final Defence Costs (FDC) not yet calculated	The guilty verdict is recorded, but the FDC have not yet been calculated.	The Authority recognises contributions value at guilty verdict as income, and recognises the outstanding contributions owed as a debt. Cash received to date against the debt is transferred from third party funds to the Authority.
FDC calculated and notified	FDCs are calculated and any unpaid contributions are collectible.	The Authority recognises the movement (up or down) between the contributions and FDC figures as income (debit or credit), and adjusts the recognised debt accordingly.
Defendant appeals	Defendant appeals guilty verdict	The Authority derecognises any income and debt previously recognised, and transfers any contributions received to date back to third party funds.
Appeal verdict – not guilty	Defendant found not guilty on appeal	As for 'Case verdict – not guilty'
Appeal verdict – guilty	Guilty verdict upheld on appeal.	As for 'Case verdict – guilty'
Debt Written off	Supplier recommends debt for write off by the Authority, and the Authority approves.	The Authority recognises a reduction in debt and a write off charge to the profit and loss.

PART II

Tables 2, 3 and 4 of this Part II are reporting requirements and must be provided in order for the Authority to fulfil its financial reporting requirements.

2. Monthly Financial Reports

The Authority requires the following core reports from the Supplier monthly and 7 calendar days following month end:

MI39 - Cumulative cash remitted summary	<p>Cumulative* summary report on cash remitted, including:</p> <ul style="list-style-type: none">- remittance ID;- remittance date;- net remittance value;- contributions/FDC cash remitted;- refunds netted;- interest paid. <p>* The report should be cumulative from the Commencement Date, with each new month's data being appended to the report.</p>
MI40 - Cumulative cash remitted at case level	<p>Detailed (to individual debtor level) cumulative* remittance report including:</p> <ul style="list-style-type: none">- Defendant's client reference and Supplier's debtor ID;- client name;- case creation date;- transaction date;- remittance ID;- remittance date;- net remittance value;- contributions/FDC cash remitted;- refunds netted;- interest paid. <p>* The report should be cumulative from the Commencement Date, with each new month's data being appended to the report.</p>
MI41 - Cumulative cash remitted at case level but not yet remitted to Authority	<p>Detailed (to individual level) report of Defendant funds remitted to the Supplier's bank but not remitted to the Authority, including:</p> <ul style="list-style-type: none">- Authority's client reference and Supplier's debtor ID;- Defendant name;- case creation date;- transaction date;- payment ID;- payment amount.
MI42 - Crystallised recognised debt book breakdown at case level	<p>Report of all recognised debt including debt fully repaid, on the final day of the month (i.e. debt that has been crystallised by a guilty verdict, and is not currently on appeal – see Accounting Treatment table above), including:</p> <ul style="list-style-type: none">- Authority's client reference and Supplier's debtor ID;- client name;- case creation date;- Sentence Order Date;- FDC issue date;- FDC payable, split between Capital and Equity, and income;

	<ul style="list-style-type: none"> - debt paid to date; - total Recognised Income; - total write off; - secured/non-secured status; - secured date, if secured; - enforcement/collection arrangements status; - case status (open or closed).
MI43 - Debt Book breakdown at case level of all crystallised debt	<p>Report of all debt including:</p> <ul style="list-style-type: none"> - Authority's client reference and Supplier's debtor ID; - debtor name; - first contribution date; - conviction status; - conviction date; - appeal status; - appeal verdict date; - crystallisation status i.e. whether convicted and not under appeal; - FDC status (issued/not issued); - contributions payable; - FDC payable, split between Capital and Equity and income; - enforcement; - handling charges; - other charges; - authorised write offs; - cleared payments received by the Supplier; - payments remitted to Authority; - refunds paid by the Supplier; - refunds netted off remittances to Authority.
MI44 - Cumulative report of all open and closed crystallised cases	<p>A report of all live and closed crystallised cases since the beginning of the scheme, including:</p> <ul style="list-style-type: none"> - Authority's client reference and Supplier's debtor ID; - created date; - Outcome date; - FDC date; - current CCO value; - secured/not-secured status; - if debt secured, secured date; - value of Secured Debt; - debt paid.
MI45 - Cumulative recognised income report showing opening and closing balances at start and end of FY	<p>A summary report of income from all schemes, showing the opening cumulative position at 1st April, the values recognised monthly, and the closing cumulative position.</p> <p>Income to be categorised as follows:</p> <ul style="list-style-type: none"> - income fee; - income fee enforcement; - Capital and Equity; - Capital Equity enforcement; and - appeals.

3. Reconciliations

The Authority will require the following reconciliations monthly and 7 calendar days following month end:

MI46 - Reconciliation report between summary remittance data and case level remittance data	A reconciliation report between the summary remittance data provided in report MI39 and the detailed remittance data provided in report MI40 above.
MI47 - Reconciliation report between recognised debt reports MI43 and MI44	A reconciliation report between recognised debt as per report MI43, and recognised debt as per report MI44 (i.e. for crystallised debt only) including: <ul style="list-style-type: none">- FDC payable (income fee and Capital and Equity);- enforcement payable;- less write offs;- less total Recognised Income.
MI48 - Overall reconciliation report between remitted cash and Recognised Income	A reconciliation report between remitted cash and Recognised Income, showing: <ul style="list-style-type: none">- total remitted;- less remitted by non-qualifying debtors;- less awaiting refund to qualifying debtors;- total Recognised Income. This reconciliation to also include a reconciliation to the total remittances as per report MI46 above.

4. Weekly report

The Authority will require the following reconciliation report weekly and within 1 Working Day following week end.

MI49 - Weekly remittance report at case level	Detailed (to individual debtor level) remittance report for that week, including: <ul style="list-style-type: none">- Defendant's client reference and Supplier's debtor ID;- client name;- case creation date;- transaction date;- remittance ID;- remittance date;- net remittance value;- contributions/FDC cash remitted;- refunds netted;- interest paid.
---	---

Annex 4 – Target Performance Levels for KPIs 1- 3

1. The target Performance Levels for KPIs 1-3 will be agreed between the Authority and Supplier on an annual basis during February/March each year for the subsequent financial year starting 1st April. The annual review of targets for KPIs 1-3 is in recognition of several factors that have the potential to change throughout the year and could therefore have an impact on reaching the target Performance Levels.
2. The target Performance Levels for Year 1 shall be agreed between the Authority and the Supplier during the implementation period. A contract change notice will be raised to add them to this schedule. The Authority expects that annual target Performance Levels for KPIs 1-3 will fall within the estimated annual target ranges shown in the table below:

KPI	Estimated Annual Target
KPI 1 Cash Collections	[Redacted]
KPI 2 Gross Secured Debt collections	[Redacted]
KPI 3 Aged Debt Collections	[Redacted]

3. The following drivers (not exhaustive) and external factors will be considered when agreeing the annual target Performance Levels.

KPI 1 – Cash Collections in each financial year

- Supplier past 12-24 month trends of ALL cash collections using data from MI report 5;
- Supplier annual Volumes of ICOs and CCOs and Appeals per month/year using last 12-24 months data from MI reports 18, 20 and 21;
- Supplier annual Average values of ICOs and CCOs and Appeals using last 12-24 months data from MI reports 18, 20 and 21;
- Supplier analysis of existing debt in debt book / existing payment arrangements collection curves from MI reports 4, 24, 25 and 26;
- Supplier annual Secured Debt cases volumes and values Paid in full and converted to cash trends using last 12-24 months data from MI report 5;
- Authority advice on known future changes to ICO or CCO values/volumes arising from legislative or policy changes or Police/Court activity which influence numbers of arrests/disposals/convictions and criminal sentencing guidelines in Crown Courts.

KPI 2 – Gross Secured Debt in each FY

- Supplier annual Volumes and annual average value trends of CCOs per month/year using past 12-24 months data from MI reports 20;
- Supplier % trends of ICOs and CCOs converted to Charging Orders using past 12-24 months MI report 22 per month/per year;
- Supplier % trends of Charge Orders that are Secured at Interim stage in past 12-24 months MI report 02 per month/per year;

- Supplier knowledge of Housing market Authority advice on known future changes to CCO values/volumes arising from legislative or policy changes.

KPI 3 – Aged Debt converted to cash in each FY

- Supplier past 12-24 month trends of cash collections from aged debt using data from MI report 5 and 6
 - Supplier analysis of existing debt in debt book / existing payment arrangements collection curves MI reports 4, 24, 25 and 26
 - Supplier analysis of leverages to collect difficult/aged debt
 - Authority advice on any changes impacting on aged debt collections
4. Agreed annual targets for KPIs 1-3 will each be profiled/projected over 12 months on a cumulative basis for the relevant reporting year. It is expected that 12 months profiling will also take account of seasonal fluctuations or known changes in Defendant propensity to pay at certain times of the year e.g. Black Friday, Christmas, main holiday periods.
 5. The latest cumulative YTD position that will be used for the purposes of monthly reporting and Service Credit scoring. A worked example is shown below.
 6. On agreement of the target Performance Level for the subsequent year, a contract change notice will be raised to add them to this schedule.

Example usage of cumulative YTD position

Annual target Performance Level for KPI 1 = [Redacted], where the Overall Admin debit score is -0.5% or 0% for the relevant reporting month.

	MTD target agreed as part of annual target negotiation	YTD target	MTD actual	YTD actual	YTD % performance (YTD actual/YTD target x100%)	Finance KPI Service Credit	Admin KPI debit	Overall Service Credit %
Apr	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
May	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
June	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
July	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Aug	[Redacted]							
Sept	[Redacted]							
Oct	[Redacted]							
Nov	[Redacted]							
Dec	[Redacted]							
Jan	[Redacted]							
Feb	[Redacted]							
March	[Redacted]							
Total	[Redacted]							

Intentionally blank.

SCHEDULE 7 - KEY PERSONNEL

At the Commencement Date the Supplier's Key Personnel are:

NAME OF KEY PERSONNEL	KEY ROLE	RESPONSIBILITIES
[Redacted]	[Redacted]	Overall Responsibility for deliverance of the LAA Contract at Board level.
[Redacted]	[Redacted]	Responsibility for Operational & Contractual performance and quality of the LAA Contract. Supports Contract Manager and works directly with Head of Crown Court Means Testing Team.
[Redacted]	[Redacted]	To assume day to day responsibility for the deliverance of the LAA Contract, utilising a suite of MI to scrutinize and help maximise collection activity. To support the Team Leader & Data Analyst and work directly with LAA Contract Manager and LAA Contract Support Manager to deliver the specifications of the LAA Contract.
[Redacted]	[Redacted]	To support a team of administrators with the daily running of the Operational processes working with the SLA and Contractual requirements and liaise directly with LAA Team Supervisor and LAA Contract Support Manager on a day to day basis on processes.
[Redacted]	[Redacted]	Responsibility for production of Financial and Performance related Management Information; holds system knowledge and able to assist in development of new/improved MI reports and produce ad hoc data.
[Redacted]	[Redacted]	Overall responsibility for ensuring Digital solutions are in place at Supplier end to receive data feeds from the Authority and has a Supplier Collection System in place that can be accessed by the Authority to case level. Transmit information back to the Authority and to

NAME OF KEY PERSONNEL	KEY ROLE	RESPONSIBILITIES
		ensure delivery of the contract. Works with LAA Digital Lead.
[Redacted]	[Redacted]	Overall responsibility for information assurance and security, including personnel security-information risk and compliance with the ISMS (Security Plan).
[Redacted]	[Redacted]	Responsible for delivery of Security Plan for the contract, reviewing and addressing IT risks and vulnerabilities and working directly with LAA Cyber Security Manager.
[Redacted]	[Redacted]	Responsible for overall GDPR compliance of contract processes and storage/retention of Authority Data held by Supplier in line with GDPR obligations.
[Redacted]	[Redacted]	Responsible for overall financial management of this contract, the accuracy of all month-end financial reports and month end reconciliation of financial reports. Liaises directly with LAA Finance Managers on any financial reporting or accuracy issues, National Office Audits, and compliance with ISAE 3402.

SCHEDULE 6 – INFORMATION ASSURANCE AND SECURITY

1 DEFINITIONS

- 1.1 Unless the context otherwise requires the following terms shall have the meanings given to them below. Other capitalised terms shall have the meanings given to them in the Terms & Conditions or Schedules in which they first appear.

"Anti-Malicious Software" means software that scans for and identifies possible Malicious Software in the ICT Environment;

"Authority Security Representative" means the Authority's representative authorised to act on information assurance and security matters.

"CJSM" means the Criminal Justice Secure Mail.

"CPA" means the NCSC Commercial Product Assurance scheme as further set out in paragraph 15.3.2 of Annex 1 (Baseline Security Requirements) to this Schedule.

"Cryptographic Policy" means the Authority's cryptographic policy as updated from time to time.

"ISMS" means the Supplier's information and management system and processes to manage information security as set out in paragraph 3.4 (Information Security Management System) of this Schedule.

"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.

"NCSC Guidance" means the NCSC End User Devices Platform Security Guidance accessible via: <https://www.ncsc.gov.uk/guidance/end-user-device-security>.

"PSN" means the Public Sector Network.

"Security Test(s)" 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.

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

2 GENERAL

- 2.1 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.

- 2.2 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.
- 2.3 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, information risk and compliance with the ISMS. The individual appointed by the Supplier, who shall be the chief security officer, chief information officer, chief technical officer or equivalent, is identified as Key Personnel and the provisions of clause B4 (Key Personnel) apply in relation to that person.
- 2.4 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, including the Supplier System.
- 2.5 Due to the constant nature of evolving informational risk threats, these requirements convey principles in lieu of an exhaustive and complete description of all possible definable requirements. The Supplier is required to create and maintain a proportional and holistic approach to information security in order to appropriately safeguard Authority Data, including Supplier-generated data or information, in relation to the fulfilment of this Contract.
- 2.6 The Supplier must continuously review and improve any products or services supplied, maintained or monitored as part of this Contract to ensure any associated controls or defences are appropriate, modern, current and proportional, in order to adequately protect and assure data or information at any point in time.
- 2.7 The Supplier must take all reasonable measures to ensure it (and any Sub-Contractors and Sub-Processors) creates and maintains an adequate information security posture, fully compliant with this schedule.
- 2.8 Due to the constant nature of evolving information risk and associated standards and guidance, a non-exhaustive list correct at the Commencement Date is included within Schedule 6 Annex 2. The Supplier must review and comply with these policies throughout its provision of the Services throughout the Term.
- 2.9 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.
- 2.10 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.

- 2.11 Any standards and Certification Requirements shown in this Schedule should include any Sub-Contractors and Sub-Processors or additional service providers that the Supplier has sub-contracted to and has access to Authority Data. Any Sub-Contractor must be Approved by the Authority, including as set out in Schedule 10 where the Sub-Contractor will be Processing Personal Data.

3 INFORMATION SECURITY MANAGEMENT SYSTEM

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

3.1.1 has been tested; and

3.1.2 complies with the requirements of paragraphs 3.3 and 3.4 of this Schedule.

- 3.2 The Supplier may not use the ISMS to Process Authority Data unless and until the Authority has issued the Supplier with an ISMS Approval in accordance with the process set out in this paragraph 3.

- 3.3 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.

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

3.4.1 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);

3.4.2 be aligned to and compliant with the relevant standards in ISO/IEC 27001: 2013 or equivalent and the Certification Requirements in accordance with paragraph 6 (Certification Requirements) of this Schedule unless otherwise Approved;

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

3.4.3.1 meet the requirements in the Contract;

3.4.3.2 are in accordance with applicable Law;

3.4.3.3 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>;

- 3.4.3.4 comply with the Security Policy Framework; Government Functional Standard GovS007: Security and Policy Framework and Cyber Essentials Plus;
 - 3.4.3.5 comply with the Baseline Security Requirements;
 - 3.4.3.6 comply with the Authority's policies, including, where applicable, the Authority's 'Information Assurance Policy' in the Information Security Policy Framework or its replacements;
- 3.4.4 address any issues of incompatibility with the Supplier's organisational security policies;
- 3.4.5 address any specific security threats of immediate relevance to Information Assets and/or Authority Data;
- 3.4.6 document:
 - 3.4.6.1 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;
 - 3.4.6.2 incident response plans, including the role of nominated security incident response; and
 - 3.4.6.3 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;
- 3.4.7 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
- 3.4.8 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 2.3 (General) above.
- 3.5 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.

- 3.6 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.
- 3.7 The Authority shall review the proposed ISMS submitted pursuant to paragraph 3.1 above and shall, within 10 Working Days of its receipt notify the Supplier as to whether it has been Approved.
- 3.8 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.
- 3.9 If the ISMS 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, within a further [Redacted] 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 [Redacted] 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).
- 3.10 Approval of the ISMS or any change to it shall not relieve the Supplier of its obligations under this Schedule 6.
- 3.11 The Supplier shall provide to the Authority, upon request, any or all ISMS documents.

4 SECURITY PLAN

- 4.1 The Supplier shall, within [Redacted] of the Commencement Date, submit to the Authority for Approval a Security Plan which complies with paragraph 4.2 below.
- 4.2 The Supplier shall effectively implement the Security Plan which shall:
 - 4.2.1 comply with the Baseline Security Requirements;
 - 4.2.2 identify the organisational roles for those responsible for ensuring the Supplier's compliance with this Schedule 6;
 - 4.2.3 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;
 - 4.2.4 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;

- 4.2.5 set out plans for transition from the information security arrangements in place at the Commencement Date to those incorporated in the ISMS;
 - 4.2.6 set out the scope of the Authority System that is under the control of the Supplier;
 - 4.2.7 be structured in accordance with ISO/IEC 27001: 2013 or equivalent unless otherwise Approved;
 - 4.2.8 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
 - 4.2.9 comply with the Security Policy Framework and Government Functional Standard GovS007:Security and Policy Framework and Cyber Essentials Plus.
- 4.3 The Authority shall review the Security Plan submitted pursuant to paragraph 4.1 above and notify the Supplier, within [Redacted] of receipt, whether it has been Approved.
- 4.4 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.
- 4.5 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 Working Days whether it has been Approved.
- 4.6 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 11 (Dispute Resolution).
- 4.7 Approval by the Authority of the Security Plan pursuant to paragraph 4.3 above or of any change to the Security Plan shall not relieve the Supplier of its obligations under this Schedule 6.

5 REVISION OF THE ISMS AND SECURITY PLAN

- 5.1 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:
- 5.1.1 any issues in implementing the Security Policy Framework and/or managing information risk;

- 5.1.2 emerging changes in Good Industry Practice;
 - 5.1.3 any proposed or actual change to the ICT Environment and/or associated processes;
 - 5.1.4 any new perceived, potential or actual security risks or vulnerabilities;
 - 5.1.5 any ISO/IEC 27001 (at least ISO/IEC 27001:2013) audit report or equivalent produced in connection with the Certification Requirements which indicates concerns; and
 - 5.1.6 any reasonable change in security requirements requested by the Authority.
- 5.2 The Supplier shall give the Authority the results of such reviews as soon as reasonably practicable after their completion, which shall include without limitation:
- 5.2.1 suggested improvements to the effectiveness of the ISMS, including controls;
 - 5.2.2 updates to risk assessments; and
 - 5.2.3 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.
- 5.3 Following the review in accordance with paragraphs 5.1 and 5.2 above 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 F6 (Change) and shall not be implemented until Approved.
- 5.4 If the Authority requires any updated ISMS and/or Security Plan to be implemented within shorter timescales than those set out in clause F6 (Change), the Parties shall thereafter follow clause F6 (Change) for the purposes of formalising and documenting the relevant Change for the purposes of the Contract.

6 CERTIFICATION REQUIREMENTS

- 6.1 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:
- 6.1.1 ISO/IEC 27001 (at least ISO/IEC 27001:2013) by a UKAS approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013); and
 - 6.1.2 The Government's Cyber Essentials Plus Scheme unless otherwise agreed with the Authority,

and shall provide to the Authority:

- 6.1.3 a copy of each such certificate of compliance and details of the scope of each such certification before the Supplier accesses the ICT Environment and/or receives, stores, processes or manages any Authority Data; and
 - 6.1.4 evidence 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.
- 6.2 The Supplier shall ensure that it and each Sub-Contractor who is responsible for the secure destruction of Authority Data:
- 6.2.1 carries out any secure destruction of Information Assets and/or Authority Data only at Supplier sites which are included within the scope of an existing certificate of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013); and
 - 6.2.2 should satisfy the Authority that their data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and
 - 6.2.3 must maintain an asset register of all Authority supplied information, data and equipment to ensure Authority assets are returned and/or deleted,
- and the Supplier shall provide the Authority with evidence of its and its Sub-Contractors compliance with the requirements set out in this paragraph 6.2 before the Supplier or the relevant Sub-Contractor may carry out the secure destruction of any Information Assets and/or Authority Data.
- 6.3 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier or any Sub-Contractor ceases to be compliant with the Certification Requirements in paragraph 6.1 of this Schedule and, on request from the Authority, shall, or procure that the relevant Sub-Contractor shall:
- 6.3.1 immediately cease access to and use of Information Assets and/or Authority Data; and
 - 6.3.2 promptly return, destroy and/or erase the Authority Data in accordance with the Baseline Security Requirements and failure to comply with this obligation is a material Default.
- 6.4 The Authority may agree to exempt, in whole or part, the Supplier or any Sub-Contractor from the requirements of this Paragraph. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Plan.
- 6.5 The Supplier must ensure that it retains a current ISO/IEC 27001 certification throughout the Contract Term. The scope of this certification must be applicable to and cover all of the systems, services and support that shall be provided to LAA under this Contract. The Supplier must be compliant with and have gained certification to

ISO/IEC 27001:2022 no later than by the end of the ISO certification transition period on [Redacted].

- 6.6 The Supplier must ensure that it retains a current Cyber Essentials Plus certification throughout the Contract Term. The scope of this certification must be applicable to and cover all of the systems, services and support that shall be provided to LAA under this Contract.
- 6.7 Where there has been an update to any standards, the Supplier must be certified to the revised version of the standard by the end of any applicable transition period.

7 SECURITY TESTING

- 7.1 The Supplier shall, at its own cost, carry out relevant Security Tests from the Commencement Date and throughout the Term, which shall include:
 - 7.1.1 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;
 - 7.1.2 an annual IT Health Check by an independent CHECK or CREST 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;
 - 7.1.3 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; and
 - 7.1.4 such other tests as are required:
 - 7.1.4.1 by any Vulnerability Correction Plans;
 - 7.1.4.2 by ISO/IEC 27001 (at least ISO/IEC 27001:2013) Certification Requirements;
 - 7.1.4.3 after any significant architectural changes to the ICT Environment;
 - 7.1.4.4 after a change to the ISMS (including security incident management processes and incident response plans) or the Security Plan; and/or
 - 7.1.4.5 and following a Breach of Security.

7.2 The Supplier shall:

7.2.1 complete all of the above Security Tests before:

7.2.1.1 the Supplier submits the Security Plan to the Authority for review; and

7.2.1.2 before the Supplier is given permission by the Authority to process or manage any Authority Data; and

7.2.2 repeat the IT Health Check not less than once every 12 months during the Term and submit the results of each such test to the Authority for review in accordance with this Paragraph.

7.3 In relation to each IT Health Check, the Supplier shall:

7.3.1 agree with the Authority the aim and scope of the IT Health Check;

7.3.2 promptly, and no later than ten (10) Working Days, following the receipt of each IT Health Check report, give the Authority a copy of the full IT Health Check report; and

7.3.3 if the IT Health Check report identifies any vulnerabilities:

7.3.3.1 prepare a Vulnerability Correction Plan for Approval which sets out in respect of each vulnerability identified in the IT Health Check report:

7.3.3.1.1 how the vulnerability will be remedied;

7.3.3.1.2 unless otherwise agreed in writing between the Parties, the date by which the vulnerability will be remedied which must be:

7.3.3.1.3 within three months of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of "medium/other";

7.3.3.1.4 within one month of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of "high/important"; and

7.3.3.1.5 within 7 Working Days of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of "critical";

7.3.3.1.6 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;

7.3.3.2 comply with the Vulnerability Correction Plan; and

7.3.3.3 conduct such further Security Tests as are required by the Vulnerability Correction Plan.

7.4 The Supplier shall ensure that any testing which could adversely affect the Supplier System shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of Security Tests shall be agreed in advance with the Authority.

7.5 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 [Redacted] after completion of each Security Test.

7.6 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:

7.6.1 upon giving reasonable notice to the Supplier where reasonably practicable to do so; and

7.6.2 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.

7.7 If the Authority carries out Security Tests in accordance with paragraph 7.6 below, 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.

7.8 If any Security Test carried out pursuant to paragraphs 7.1 or 7.6 reveals any:

7.8.1 vulnerabilities during any accreditation process, the Supplier shall track and resolve them effectively; and

7.8.2 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 5.3 and 5.4 above, 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.

7.9 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 7.8.2, the Supplier is not in breach of the Contract to the extent that it can be shown that such breach:

7.9.1 has arisen as a direct result of the Authority unreasonably withholding Approval to the implementation of such proposed changes; and

7.9.2 would have been avoided had the Authority Approved the implementation of such proposed changes.

7.10 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.

7.11 If any repeat Security Test carried out pursuant to paragraph 7.7 reveals an actual or potential Breach of Security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default.

7.12 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 2.3 (General) above confirming that having made due and careful enquiry:

7.12.1 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

7.12.2 the Supplier is confident that its security and risk mitigation procedures in relation to Information Assets and Authority Data remain effective.

8 SECURITY AUDITS AND COMPLIANCE

8.1 The Authority and its Authorised Security 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.

8.2 If ISO/IEC 27001 (at least ISO/IEC 27001:2013 certification or equivalent is provided; the ISMS shall be independently audited in accordance with ISO/IEC 27001 (at least ISO/IEC 27001:2013). The Authority and its Authorised Security Representatives shall,

where applicable, be granted access to the Supplier and Sub-Contractor Premises for this purpose.

- 8.3 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 (at least ISO/IEC 27001:2013), 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).
- 8.4 If, as a result of any such independent audit as described in paragraph 8.3 above the Supplier is found to be non-compliant with any applicable principles and practices of ISO/IEC 27001 (at least ISO/IEC 27001:2013), 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 compliant and shall reimburse the Authority in full in respect of the costs obtaining such an audit.

9 SECURITY RISKS AND BREACHES

- 9.1 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.
- 9.2 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.
- 9.3 Without prejudice to the security incident management processes and incident response plans set out in the ISMS, upon becoming aware of any Breach of Security or attempted Breach of Security, the Supplier shall:
- 9.3.1 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:
 - 9.3.1.1 minimise the extent of actual or potential harm caused by any Breach of Security;
 - 9.3.1.2 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;
 - 9.3.1.3 mitigate against a Breach of Security or attempted Breach of Security; and

- 9.3.1.4 prevent a further Breach of Security or attempted Breach of Security in the future resulting from the same root cause failure;
- 9.3.2 provide to the Authority 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
- 9.3.3 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.

- 9.4 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.

10 IT ENVIRONMENT

- 10.1 At all times the Supplier must take into account the "State of the Art" (as defined in Article 32 of UK GDPR) and ensure that the Supplier System, its software and processes are maintained to a standard that provides adequate protection against new and emerging threats. To that end the Supplier shall ensure that the Supplier System:
 - 10.1.1 functions in accordance with Good Industry Practice for protecting external connections to the internet;
 - 10.1.2 functions in accordance with Good Industry Practice for protection from malicious code;
 - 10.1.3 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;
 - 10.1.4 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
 - 10.1.5 uses the latest versions of anti-virus definitions, firmware and software available from industry accepted anti-virus software vendors.

- 10.2 Notwithstanding paragraph 10.1 above, 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.
- 10.3 All costs arising out of the actions taken by the Parties in compliance with paragraphs 9.2 (Security Risks and Breaches), 9.3 (Security Risks and Breaches) and 10.2 (IT Environment) above shall be borne by:
- 10.3.1 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
- 10.3.2 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.

11 VULNERABILITIES AND CORRECTIVE ACTION

- 11.1 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.
- 11.2 The severity of any vulnerabilities shall be categorised by the Supplier as "critical", "high/important" and "medium/other" according to the agreed method in the ISMS and using any appropriate vulnerability scoring systems including:
- 11.2.1 the "National Vulnerability Database" "Vulnerability Severity Ratings": "High", "Medium" and "Low" respectively (these in turn are aligned to CVSS scores as set out by NIST at <http://nvd.nist.gov/cvss.cfm>); and
- 11.2.2 Microsoft's "Security Bulletin Severity Rating System" ratings "Critical", "Important", and the two remaining levels ("Moderate" and "Low") respectively.
- 11.3 The Supplier shall procure the application of security patches to vulnerabilities in the ICT Environment and ISMS within:
- 11.3.1 seven (7) days after the public release of patches for those vulnerabilities categorised as "critical";
- 11.3.2 thirty (30) days after the public release of patches for those vulnerabilities categorised as "high/important"; and
- 11.3.3 sixty (60) days after the public release of patches for those vulnerabilities categorised as "medium/other".

11.4 The timescales for applying patches to the vulnerabilities set out in paragraph 9.3 above may be extended where:

11.4.1 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 11.3 above;

11.4.2 the application of a security patch in respect of a vulnerability categorised as "critical" or "high/important" adversely affects the Supplier's ability to deliver the Services, in which case the Supplier shall be granted an extension to the timescales of 5 days, provided that the Supplier had followed and continues to follow any security patch test plan agreed with the Authority; or

11.4.3 the Authority agrees a different maximum period after a case-by-case consultation with the Supplier in accordance with the processes defined in the Security Plan.

11.5 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:

11.5.1 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

11.5.2 otherwise agreed with the Authority in writing.

11.6 The Supplier shall:

11.6.1 implement a mechanism for receiving, analysing and acting upon threat information provided by NCSC, or any other competent central Government body;

11.6.2 promptly notify NCSC of any actual or sustained attempted Breach of Security;

11.6.3 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;

11.6.4 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;

11.6.5 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 Security Plan;

- 11.6.6 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;
 - 11.6.7 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;
 - 11.6.8 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
 - 11.6.9 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 ICT Environment (to the extent this is within the control of the Supplier) and provide initial indications of possible mitigations.
- 11.7 If the Supplier is unlikely to be able to mitigate any vulnerability within the timescales in paragraph 11.3 or 11.4 above, the Supplier shall notify the Authority immediately.
 - 11.8 Any failure by the Supplier to comply with paragraph 11.3 above shall constitute a Material Breach.

12 SUB-CONTRACTS

- 12.1 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.

13 MALICIOUS SOFTWARE

- 13.1 The Supplier shall install and maintain Anti-Malicious Software or procure that Anti-Malicious Software is installed and maintained on any part of the ISMS which may process Authority Data and ensure that such Anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the ISMS to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the ISMS, to identify, contain the spread of, and minimise the impact of Malicious Software.
- 13.2 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

13.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 13.2 above shall be borne by the Parties as follows:

13.3.1 by the Supplier where the Malicious Software originates from:

13.3.1.1 the Supplier Software;

13.3.1.2 the Third Party Software supplied by the Supplier; or

13.3.1.3 the Authority Data whilst the Authority Data is or was under the control of the Supplier,

unless, in the case of the Authority Data only, the Supplier can demonstrate that such Malicious Software was present in the Authority Data and not quarantined or otherwise identified by the Authority when the Authority provided the Authority Data to the Supplier; and

13.3.2 by the Authority, in any other circumstance.

ANNEX 1 - BASELINE SECURITY REQUIREMENTS

14 SECURITY CLASSIFICATIONS AND CONTROLS

- 14.1 The Supplier shall, unless otherwise Approved by the Authority, only have access to and handle Information Assets and Authority Data that are classified under the Government Security Classifications Scheme as OFFICIAL.
- 14.2 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.'
- 14.3 The Supplier shall apply the minimum security controls required for OFFICIAL information and OFFICIAL-SENSITIVE information as described in Cabinet Office guidance, currently at: [May-2018_Government-Security-Classifications-2.pdf \(publishing.service.gov.uk\)](#).
- 14.4 Save as set out below in relation to clients/debtors, the Supplier shall ensure that any correspondence that is sent under this Contract containing OFFICIAL-SENSITIVE material (for example, interactions with solicitors and the Legal Aid Agency) is only sent by DX Secure or Royal Mail Special Delivery and not by email except to @gov accounts or to a Criminal Justice Secure Mail account. For correspondence that is sent under this Contract to clients/debtors, the Supplier must give due regard to the content of correspondence and whether additional precautions should be taken (for example, a Capital Contribution Order is unlikely to be 'OFFICIAL SENSITIVE' but occasionally a complex Complaint response may be so).
- 14.5 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.
- 14.6 Additional controls may be required by the Authority and any accreditor where there are aspects of data aggregation.

15 END USER DEVICES

- 15.1 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:
 - 15.1.1 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 140-3 standard or equivalent, unless Approved;

- 15.1.2 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 140-3 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.
- 15.2 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.
- 15.3 Unless otherwise Approved, when Authority Data resides on a mobile, removable or physically uncontrolled device, it shall be:
- 15.3.1 the minimum amount that is necessary to achieve the intended purpose and should be anonymised if possible;
- 15.3.2 stored in an encrypted form meeting the FIPS 140-3 standard or equivalent and using a product or system component which has been formally assured through a recognised certification process of NCSC to at least foundation grade, for example, those previously assured under the NCSC Commercial Product Assurance scheme (CPA) or equivalent, unless otherwise Approved;
- 15.3.3 protected by an authentication mechanism, such as a password; and
- 15.3.4 have up to date software patches, anti-virus software and other applicable security controls to meet the requirements of this Schedule.
- 15.4 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 NCSC Guidance or equivalent.
- 15.5 Where the NCSC 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 NCSC Guidance, this should be agreed in writing with the Authority on a case by case basis.

16 DATA STORAGE, PROCESSING, MANAGEMENT, TRANSFER AND DESTRUCTION

- 16.1 In addition to the obligations on the Supplier set out Clause E2 (Data Protection and Privacy) in respect of Processing Personal Data and compliance with the Data Protection Legislation, 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.

- 16.2 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 in accordance with clause E2 (Data Protection and Privacy).
- 16.3 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.
- 16.4 The Supplier shall ensure that any electronic transfer of Authority Data:
 - 16.4.1 protects the confidentiality of the Authority during transfer through encryption suitable for the impact level of the data;
 - 16.4.2 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
 - 16.4.3 prevents the repudiation of receipt through accounting and auditing.
- 16.5 The Supplier shall:
 - 16.5.1 protect Authority Data, including sensitive 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;
 - 16.5.2 ensure that any OFFICIAL SENSITIVE information and all Personal Data is encrypted in transit and when at rest when stored away from the Supplier's controlled environment;
 - 16.5.3 on demand, provide the Authority with all Authority Data in an agreed open format;
 - 16.5.4 have documented processes to guarantee availability of Authority Data if it ceases to trade;
 - 16.5.5 securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority;
 - 16.5.6 securely destroy all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in the Contract and, in the absence of any such requirements, as directed by the Authority;
 - 16.5.7 securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority;

16.5.8 ensure that all material used for storage of Confidential Information is subject to controlled disposal and the Supplier shall:

16.5.8.1 destroy paper records containing protected Personal Data by incineration, pulping or shredding so that reconstruction is unlikely; and

16.5.8.2 dispose of electronic media that has been used for the processing or storage of protected Personal Data through secure destruction, overwriting, erasure or degaussing for re-use.

17 NETWORKING

17.1 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 NCSC, 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.

17.2 The Authority requires 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, is at least compliant with Good Industry Practice.

17.3 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.

18 REMOTE/ HYBRID WORKING

18.1 The Authority may during the Term permit the Supplier to carry out Services under the Contract from alternative locations other than the Premises if the Supplier can demonstrate to the Authority's satisfaction that they can continue to comply with paragraphs 10.1-10.3 (IT Environment) of this Schedule 6 as well as any additional requirements the Authority may specify to ensure appropriate levels of security are maintained.

18.2 In the event that a hybrid / remote working model is sought by the Supplier and agreed by the Authority, the Supplier must ensure, and the Authority must agree, that remote working locations are suitable and the model complies with the Law and other requirements and standards specified under this Contract.

18.3 In addition to the requirement set out in paragraph 18.2 above, the Supplier must continue to:

18.3.1 demonstrate to the Authority's continued satisfaction that the IT infrastructure used to connect to any servers or systems remotely (and which forms part of

the Supplier System) is secure and protects Authority Data from any unauthorised access, Processing, loss or theft, and that the confidentiality, integrity and availability of the Authority Data is adequately protected;

18.3.2 demonstrate to the Authority's continued satisfaction that it has sufficient guidance and policies that reflect working from a home or alternative location environment. This should include, as a minimum, Staff awareness of the risks involved and policies and guidance in relation to handling data breaches remotely. This may also include having a documented register that specifies what assets are being processed outside of the office environment;

18.3.3 conduct regular audits of Staff compliance with paragraphs 18.3.1 and 18.3.2 above and share the findings with the Authority on request;

18.3.4 deliver information security training to all Staff working under this Contract that adequately addresses compliance and risks associated with working at home or an alternative location;

18.3.5 have a leavers policy which details the process to be followed to ensure recovery of assets from members of staff working remotely or in an alternative location; and

18.3.6 ensure that staff working under this Contract will not use any personal devices to deliver the Services under the Contract.

19 SECURITY ARCHITECTURES

19.1 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 NCSC certification or equivalent for all bespoke or complex components.

19.2 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.

19.3 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. Staff 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.

20 DIGITAL CONTINUITY

20.1 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, in accordance with any information handling procedures set out in ISO/IEC 27001:2013; Government Functional Standard 007: Security and Information Security Policy Framework principles or its replacements.

21 PERSONNEL VETTING AND SECURITY

- 21.1 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 the BPSS or BS7858 or equivalent.
- 21.2 All Staff who have logical or physical access to Information Assets and/or Authority Data classified at a higher level than OFFICIAL, or all Staff who have unsupervised access to server rooms or have privileged admin user access to bulk data at OFFICIAL level require 'SC' clearance. The Supplier shall obtain the specific Government clearances that are required for access to such Information Assets and/or Authority Data.
- 21.3 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.
- 21.4 The Supplier shall procure that all Staff comply with the Government Functional Standard 007: Security and Security Policy Framework principles, obligations and policy priorities stated therein, including requirements to manage and report all security risks in relation to the provision of the Services.
- 21.5 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.
- 21.6 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.

22 IDENTITY, AUTHENTICATION AND ACCESS CONTROL

- 22.1 The Supplier shall operate a robust role-based access control regime, including network controls, to ensure all Staff using, administering and 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*', Staff using, administering and maintaining shall be allowed access only to those parts

of the ICT Environment they require. The Supplier shall retain an audit record of accesses and Staff using, administrating and maintaining the ICT Environment and disclose this to the Authority upon request.

- 22.2 The Supplier shall ensure that Staff who use the Authority System actively confirm annually their acceptance of the Authority's acceptable user policy.

23 PHYSICAL MEDIA

- 23.1 The Supplier shall ensure that:

23.1.1 all OFFICIAL information is afforded physical protection from internal, external and environmental threats commensurate with the value to the Authority of that information;

23.1.2 all physical components of the Supplier System are kept in secure accommodation which conforms to the Security Policy Framework and NCSC standards and guidance or equivalent;

23.1.3 all physical media holding OFFICIAL information is handled in accordance with the Functional Standard for Government GovS 007: Security and NCSC standards and guidance or equivalent; and

23.1.4 all Information Assets and Authority Data held on paper are:

23.1.4.1 kept secure at all times and 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;

23.1.4.2 only processed in an office location and are not processed at home or an alternative location; and

23.1.4.3 transferred by post adhering to any standards the Authority may specify or transferred in person only where necessary, in secure bags or cases kept on the person at all times in transit.

24 AUDIT AND MONITORING

- 24.1 The Supplier shall implement effective monitoring of its information assurance and security obligations in accordance with NCSC [Security policy framework: protecting government assets - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/policies/protecting-government-assets). 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 (as a minimum) include:

24.1.1 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, regular reports and alerts giving details of access by Staff 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

24.1.2 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. The Parties shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

24.2 The retention period for audit records and event logs must be agreed with the Authority and documented in the Security Plan.

25 SECURE ARCHITECTURE

25.1 The Supplier shall design the ICT Environment (to the extent that it is within the control of the Supplier) in accordance with:

25.1.1 the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main>;

25.1.2 the NCSC "Bulk Data Principles", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main>; and

25.1.3 the NSCS "Cloud Security Principles", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles> and which are summarised below:

25.1.4 "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;

25.1.5 "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;

- 25.1.6 "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;
- 25.1.7 "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Services and information within it;
- 25.1.8 "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;
- 25.1.9 "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Staff have access to Authority Data and/or the Authority System that those personnel be subject to appropriate security screening and regular security training;
- 25.1.10 "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;
- 25.1.11 "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Sub-Contractors and other suppliers;
- 25.1.12 "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Authority to securely manage the Authority's use of the Service;
- 25.1.13 "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;
- 25.1.14 "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;
- 25.1.15 "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any IT system which is used for administration of a cloud service will have highly privileged access to that service;
- 25.1.16 "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Authority with the audit records it needs to monitor access to the Service and the Authority Data held by the Supplier and/or its Sub-Contractors;

25.1.17 "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Staff on the safe and secure use of the ISMS.

ANNEX 2 - INFORMATION SECURITY AND ASSURANCE STANDARDS AND GUIDANCE

The list below is a non-exhaustive list of standards and guidance location(s) the Supplier is required to review and appropriately consider and integrate into their Services.

This list is supplementary to, or may be superseded by, other published commercial best practices/guidance, National Cyber Security Centre (NCSC) guidance or Authority guidance/instructions.

This list is correct at the Commencement Date and may be revised from time to time.

Guidance & Policies	Location
Ministry of Justice Data Sharing Principles	link
Technical Controls Summary (technical and security controls recommended by Cabinet Office)	link
LAA Departmental Retention Periods	link
Ministry of Justice Security Guidance	link
APIs and System Integration Standard	link
Email Security Standard	link
Digital Service Standard	link
Open Standards for Government	link
UK HMG Technology Code of Practice	link
Minimum Cyber Security Standard	link
ISO/IEC 20000	link
ISO/IEC 27001	link
ISO/IEC 27002	link
Cyber Essentials Plus	link
National Cyber Security Centre (guidance)	link

Guidance & Policies	Location
National Cyber Security Centre (risk management)	link
National Cyber Security Centre (CHECK scheme)	link
National Cyber Security Centre (end-user device reset procedures)	link
National Cyber Security Centre (secure sanitisation of storage media)	link
National Cyber Security Centre (Cloud Security Principle 2: Asset Protection and Resilience - Data Destruction)	link
Payment Card Industry Data Security Standard (Data Destruction)	link
HMG Security Policy Framework	link
HMG (Cabinet Office and NCSC) Guidance on Security Technology at OFFICIAL	link
National Cyber Security Centre (NCSC) Guidance	link
Government Security Classifications	link
HMG Cloud Security Guidance and Cloud Security Principles	link link
Functional standard for Government GovS007	link

SCHEDULE 5 – SUPPLIER AND THIRD PARTY SOFTWARE

Supplier Software comprises the following:

<u>Software</u>	<u>Supplier (if Affiliate of the Supplier)</u>	<u>Purpose</u>	<u>No. of Licences</u>	<u>Restrictions</u>	<u>No. of copies</u>	<u>To be deposited in escrow?</u>
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted] d]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted] d]	[Redacted]
[Redacted]]	[Redacted]	[Redacted]	[Redacted]]	[Redacted]	[Redacted] d]	[Redacted]
[Redacted]	[Redacted] d]	[Redacted]	[Redacted]	[Redacted]	[Redacted] d]	[Redacted]
[Redacted]]	[Redacted]	[Redacted]	[Redacted]]	[Redacted]	[Redacted] d]	[Redacted]

Third Party Software comprises the following:

[illegible]

SCHEDULE 4 – COMMERCIALLY SENSITIVE INFORMATION

1. Without prejudice to the Authority's general obligation of confidentiality, the Parties acknowledge the Authority's obligation to publish this Contract in accordance with the Law, and that the Authority may have to disclose information contained in and/or relating to the Contract following a Request for Information pursuant to clause E5 (Freedom of Information).
2. In this Schedule 4, the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive, the disclosure of which may cause the Supplier significant commercial disadvantage or material financial loss if it was published pursuant to clause E4.2 (Confidential Information), and/or disclosed pursuant to clause E5 (Freedom of Information).
3. In addition, the Parties have sought to identify when any relevant information will cease to fall into the category of Commercially Sensitive Information.

<u>SUPPLIER'S COMMERCIALLY SENSITIVE INFORMATION</u>	<u>DATE</u>	<u>DURATION OF CONFIDENTIALITY</u>
Pricing	[Redacted]	[Redacted]
Operational Solution Details	[Redacted]	[Redacted]

SCHEDULE 3 – SUPPLIER SOLUTION

[Redacted]

SCHEDULE 2 – PRICING AND PAYMENT

1. DEFINITIONS

- 1.1 Unless the context otherwise requires, the following words and expressions shall have the following meanings. Other capitalised terms shall have the meanings given to them in the Terms & Conditions or Schedule in which they first appear.

"Additional Legal Costs"	means those costs for ad hoc legal advice and support not included in Solicitors' Fees – for example costs in respect of defending appeals.
"Allowable Enforcement Costs"	means all enforcement costs with the exception of those fees listed in the Taking Control of Goods (Fees) Regulations 2014 – Fees Recoverable under Regulation 4.
"Additional Transition Costs"	means those costs incurred specifically in transitioning live cases from the Outgoing Supplier for which there is not an agreed fixed price.
"Contract Year"	means each consecutive twelve (12) month period during the Term commencing on the Service Commencement Date and thereafter beginning on the anniversary of the Service Commencement Date.
"Court Fees"	means the fees set by statute in respect of enforcement and related proceedings;
"Enforcement Costs"	means the costs associated with enforcing a case and comprise Enforcement Fees, Solicitor's Fees and Court Fees.
"Enforcement Fees"	means the fees set in law as described in paragraphs 2.12 and 2.13.
"High Court Writ"	means a court order that allows High Court Enforcement Officers (HCEOs) the powers to access premises and seize assets to sell and repay debts owed.
"Service Costs"	means the total value of the Unit of Work Prices completed in the relevant monthly invoice period.
"Solicitors' Fees"	means the fees chargeable by the Supplier for obtaining legal advice and support in connection with routine enforcement activity.
"Third Party Debt Order"	means a court order to 'freeze' money held by a third party, such as the Defendant's bank.

"Unit(s) of Work"	means a particular stage of case work and all of the associated activities required to complete that work.
"Unit of Work Price"	means the unit cost of carrying out all of the work associated with a particular Unit of Work.

Part 1 – Calculation of the Price

2. ELEMENTS OF THE PRICE

- 2.1 The Price payable to the Supplier by the Authority for the full and proper performance by the Supplier of its obligations under this Contract is calculated in accordance with this Schedule. For the avoidance of doubt, no further amounts shall be payable by the Authority in respect of such performance.
- 2.2 All prices are fixed meaning that they are not subject to change, unless in accordance with paragraph 4, Indexation or paragraph 5, Annual Volume Review & Price Review, below. All prices exclude VAT.
- 2.3 The Price payable for the Services covers:
- (a) Service Costs, based on the Unit of Work;
 - (b) Enforcement Costs;
 - (c) any Additional Legal Costs; and
 - (d) Additional Transition Costs.

Service Costs

- 2.4 Service Costs are based on the fixed rates for the Units of Work carried out by the Supplier. The Unit of Work Price covers all costs involved in handling a specific stage of case work, as detailed in Schedule 1, including the administration associated with enforcement, should enforcement become necessary.
- 2.5 The Unit of Work Prices payable to the Supplier by the Authority for the individual Units of Work will be in accordance with the prices set out in Table 1 in Appendix 1 to this Schedule 2. A full breakdown of the costs comprised in each fixed rate for a specific type of Unit of Work is at Appendix 2 to this Schedule 2.
- 2.6 The Unit of Work Price will become payable on completion of the applicable individual Unit of Work.
- 2.7 Due to the nature of the case work process, not every Unit of Work will apply to every case. These exemptions and a flowchart showing the various different routes that a case can take are at Appendix 3 to this Schedule 2.

Enforcement Costs

- 2.9 That part of the Price payable for Enforcement Costs has three elements - Court Fees, Solicitors' Fees, and Enforcement Fees.
- 2.10 Court Fees are set by legislation. The full list of Court Fees are currently set out in the Civil Proceedings Fees Order 2008 (as amended).

- 2.11 A fixed price is payable to the Supplier by the Authority in respect of the Solicitors' Fees incurred during the enforcement process. Solicitors' Fees will be calculated on a per case basis as set out in Table 2 in Appendix 1 to this Schedule 2.
- 2.12 Enforcement Fees are set in law in accordance with:
- the Taking Control of Goods (Fees) Regulations 2014;
 - Charging Orders Act 1979, Civil Procedure Rules Part 73;
 - High Court Enforcement Officers Regulations 2004;
 - Land Registry Fee Order 2021;
 - Attachment of Earnings Act 1971, Civil Procedure Rules Part 89;
 - Civil Procedure Rules, Part 45 (Fixed Costs).
- 2.13 Enforcement Fees will be charged to the Authority and repaid in accordance with paragraph 2.14 below once collected from the Defendant, with the exception of those listed in the Taking Control of Goods (Fees) Regulations 2014 – Fees Recoverable under Regulation 4. These fees are payable by the Defendant only. The Supplier shall not be entitled to any payment from the Authority even if the Supplier is unable to recover such Fees from the Defendant.
- 2.14 Any proceeds collected from the Defendant towards their debt where it is less than the amount outstanding, must be allocated in accordance with Regulation 13 (Application of proceeds where less than the amount outstanding) of the Taking Control of Goods (Fees) Regulations 2014.

Additional Legal Costs

- 2.15 In the event that the administration and enforcement of a case involves additional legal work that cannot be accurately scoped at the start of a case, such as any additional work associated with Charging Orders, the Price may include the cost of this additional work. Any Additional Legal Costs will be calculated on the basis of the hourly rates set out in Table 3 of Appendix 1 to this Schedule 2.
- 2.16 In the event of a change of Supplier, where the courts are required to be notified of that change of Supplier or Supplier's solicitor, costs should be calculated on the basis of the hourly rates set out in Table 3 of Appendix 1 to this Schedule 2.
- 2.17 Where Additional Legal Costs reach or are expected to exceed [Redacted] for a particular case, the Supplier must seek permission from the Authority to proceed. This should be done via email to the Authority CM and any permission to proceed should be retained for audit purposes and presented with the associated invoice. The Authority may introduce additional spend limits requiring further approval where considered necessary.

Additional Transition Costs

- 2.18 In the event that the Supplier will incur Additional Transition Costs that is, any costs specifically attributable to transitioning live cases that have been transferred from the Outgoing Supplier, and which are not within the scope of the Unit of Work Prices, the Supplier is to notify the Authority in writing as soon as any such Costs are identified and in any event prior to incurring them so that the Authority may understand the basis of these proposed Additional Transition Costs and, the Parties acting

reasonably with regard to the level of such Additional Transition Costs, approve them.

- 2.19 Any proposed Additional Transition Costs must be based on the rates in this Schedule 2 and any associated statutory fees, as applicable. The Supplier must take reasonable steps to mitigate Additional Transition Costs and provide evidence of such Costs when the relevant invoice is raised and reference the approval given by the Authority.

3. EXPENSES

- 3.1 Unless specifically referred to in the Contract, the Authority shall not be liable for any expenses incurred by the Supplier in connection with the delivery of the Services or the performance of its obligations under the Contract.

4. INDEXATION

- 4.1 With the exception of Court Fees and Enforcement Fees which are set nationally, the Unit of Work Prices, Solicitors' Fees and Additional Legal Costs are indexed in accordance with the Office for National Statistics Consumer Price Index (CPI) on the first anniversary of the Service Commencement Date and on each anniversary of the Service Commencement Date thereafter.
- 4.2 Where the annual rate of inflation is 2.1% or less, the fixed rates remain unchanged for the following Contract Year. In the event that the annual rate of inflation is higher than 2.1%, then the fixed rates shall be adjusted to reflect the relevant rate minus the 2.1% threshold and subject to a 5% cap.
- 4.3 Where indexation applies, the relevant adjustment shall be determined by multiplying the relevant amount or sum by the percentage increase or changes in the Consumer Price Index published for the 12 months ended on the 31 December immediately preceding the relevant adjustment date.

Worked examples (dates and figures are for illustration purposes only)-

Fixed rate for Unit of Work for Issue ICO (Year 2) is

[Redacted] Contract Year runs from 1 January

Inflation for Jan 2023 to Dec 2023 as per the CPI is

[Redacted] Since the rate of inflation > [Redacted]

Revised rate for Units of Work for ICO Cases = [Redacted]

Fixed hourly rate for Solicitors' Fees (Year 4) is [Redacted]

Contract Year runs from 1 January

Inflation for Jan 2025 to Dec 2025 as per the CPI is

[Redacted] Since the rate of inflation > [Redacted]

[Redacted].

Revised rate for Solicitors' Fees = [Redacted]

- 4.4 Except as set out in this paragraph 4, no costs, expenses, fees and/or charges will be adjusted to take account of any inflation, change to exchange rates, any change to interest rates or any other factor or element which might otherwise increase the cost to the Supplier and/or its Sub-Contractors of performing its obligations under this Contract.

5. **ANNUAL VOLUME REVIEW AND PRICE REVIEW**

- 5.1 The Authority will review the volumes of work provided to the Supplier annually. Such review will commence ten (10) months after the Service Commencement Date and thereafter annually on the anniversary of the Service Commencement Date. The review will be based on case volumes for the preceding period (i.e. ten (10) months' data for the first review period and thereafter twelve (12) months' data) and include any assumptions made by the Supplier and the Authority regarding the forecast volumes and trends in relation to the relevant review period. As part of the review process, the Supplier is required to maintain a detailed (open book) profit and loss document over the Contract Term, showing a breakdown of income, and direct and indirect costs for all types of cases per Contract Year.
- 5.2 If the annual volume review identifies that all issued ICOs, CCOs and K&E Checks have fallen or are likely to fall below a level sufficient to maintain the viability of the Contract as identified in Appendix 4 to this Schedule 2, then a Price Review will be triggered. Similarly, if the volumes increase to a level as identified in Appendix 4 to this Schedule 2 and where it may be considered that the Supplier's profit rate has increased beyond [Redacted] a Price Review will be triggered. Both Parties shall use all reasonable endeavours to agree a new Contract Price that maintains the viability of the Contract or reduce the profit level back to [Redacted] to take effect from the annual anniversary of the Service Commencement Date. This review will take a holistic approach, taking into account all Unit of Work Prices paid to date and the overall turnover on the Contract compared with that predicted.

Part 2 – Payment

6. **PAYMENTS BY THE AUTHORITY TO THE SUPPLIER**

- 6.1 Invoices may be submitted monthly to cover:
- 6.1.1 Service Costs;
 - 6.1.2 Allowable Enforcement Costs;
 - 6.1.3 Additional Legal Costs;
 - 6.1.4 Service Credits and/or Service Debits
 - 6.1.5 Interest on Defendant Refunds; and
 - 6.1.6 Additional transition costs.
- completed/incurred in the month covered by the invoice.
- 6.2 Any Service Credits and/or Service Debits accruing in the relevant invoice period shall be calculated in accordance with Schedule 8 (Performance, Management and Reporting) and reflected in the invoice.
- 6.3 The Supplier shall 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 will not, at any later date, be liable to pay the Supplier any additional VAT.

- 6.4 All invoices must be supported by case-level data showing for each invoiced item the relevant Authority MAAT reference number, surname, type of cost, and the date the relevant cost was incurred by the Supplier.
- 6.5 In parallel, the Supplier must ensure that its Collection System is up-to-date and shows the dates and types of enforcement action taken, relevant case notes, together with copies of any supporting evidence such as copies of letters sent out (including the date sent out if not shown on the letter), and copies of evidence from solicitors in connection with any enforcement action taken. The associated Enforcement Costs shall be added to the Defendant's debt and paid back to the Authority once recovered from the Defendant.

7. PAYMENTS FROM THE SUPPLIER

- 7.1 The Supplier shall pay all monies received from Defendants in respect of Contribution Orders and Enforcement Fees into a sole and dedicated Authority account separate from all other monies administered by the Supplier. No other monies except those monies in respect of the payments to the Authority from Defendants must be paid into this account.
- 7.2 The Supplier shall remit all monies collected from Defendants to the Authority on a weekly basis, no later than five (5) Working Days after collection, save that the Supplier shall retain cheque payments from Defendants in its client account for up to five (5) Working Days until cleared and then remit the relevant payment to the Authority. This will ensure that no payment made by a Defendant to the Authority is dishonoured, however, if any payment following this period of time is reversed, the Supplier will be liable to honour the payment.
- 7.3 Each remittance shall be paid via the BACS payment system (as notified to the Supplier), and shall be accompanied by a financial report detailing the following information for each payment:
- 7.3.1 full name;
 - 7.3.2 Authority MAAT reference number;
 - 7.3.3 Supplier unique ID;
 - 7.3.4 amount being remitted to the Authority.
- 7.4 In addition, the financial report shall include a statement of the amount being held awaiting clearance together with details of which Defendants are affected.

8. DEFENDANT REFUNDS

- 8.1 The Authority will pay the [Redacted] interest added to refunds made to Defendants in the event of overpayment or acquittal. The total interest costs for the relevant month must be included on the invoice and accompanied by the relevant case data, being the Authority MAAT reference number, Defendant surname, the amount of interest paid at [Redacted] and the date paid to the Defendant. The Supplier's Collection System must also show that the Defendant refund has been Approved by the Authority, the amount of the refund, the amount of interest paid and date this was sent, together with a copy of the covering dated letter giving a breakdown of how the refund was calculated.

- 8.2 Where the value of any Defendant refund is significantly greater than the contributions collected and their insufficient reserves are held in the holding account, the Supplier may make a request that the Authority extends the five (5) day period for making the refund. Any such requests to extend the timescale for making a refund must be made on a weekly basis, with each such request being supported by a full case breakdown and explanation of the extension required. Subject to its reasonable verification of any such requests, the Authority shall allow the Supplier longer than five (5) Working Days to issue a Defendant refund.

9. FORM OF INVOICE AND SUBMISSION

- 9.1 The Supplier shall submit all invoices to the Authority on or before the tenth (10th) Working Day following the end of the month to which they relate.
- 9.2 The Supplier shall submit [Redacted] each month. The first will cover Allowable Enforcement Costs, Additional Legal Costs and the second will cover Service Costs, service credits, service debits and interest on Defendant refunds.
- 9.3 For Additional Transition Costs which the Authority has agreed to pay, the Supplier should contact the Contract Manager to discuss which invoice these are to be included on.
- 9.4 The Supplier shall work with the Authority and its nominated agent to agree an electronic invoice format which meets the requirements of a Valid Invoice as further detailed in clause C1.5 of the Terms & Conditions.
- 9.5 Subject to clause C1.5, the Authority shall pay all undisputed sums due to the Supplier within thirty (30) days of receipt of a Valid Invoice. The Supplier shall send all invoices to the Authority's finance team via secure file transfer in the first instance. Where secure file transfer is not available, they should be sent via email to the following email address:

[redacted]

- 9.6 If the Authority pays the Supplier prior to the submission of a Valid Invoice, this payment shall be on account of and deductible from the next payment to be made to the Supplier.
- 9.7 Any late payment of undisputed Valid Invoices by the Authority will be subject to interest at the annual rate of a maximum of [Redacted] above the base rate from time to time of the Bank of England. The Parties agree that this paragraph 9.76 is a substantial remedy for late payment of any sum payable under this Agreement for the purposes of the Late Payment of Commercial Debts (Interest) Act 1998.

10. VAT INDEMNITY

- 10.1 The Supplier shall indemnify 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.
- 10.2 Any amounts due under this paragraph 10 shall be paid by the Supplier to the Authority not less than five (5) Working Days before the date upon which the relevant tax or other liability is payable by the Authority.

11. MINIMUM QUANTITIES

- 11.1 The Authority does not guarantee any minimum quantities/volumes associated with any part of this Contract. Any volumes provided are for information only.

APPENDIX 1 TO SCHEDULE 2
PRICING TABLES

Table 1 – Service Costs

<u>Unit of Work Reference</u>	<u>Unit of Work</u>	<u>Unit of Work Price</u>					
		<u>Year 1 (£)</u>	<u>Year 2 (£)</u>	<u>Year 3 (£)</u>	<u>Year 4 (£)</u>	<u>Option Year 5 (£)</u>	<u>Option Year 6 (£)</u>
1	Set up new account and issue ICO collections letter	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
2	Closure of ICO before paid in full due to i) reassessed to NIL from start, ii) withdrawn or iii) written off or refunded/closed due to acquittal	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
3	ICO debt secured	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
4A	ICO paid in full where debt has been secured	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
4B	ICO paid in full where debt was not secured	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
5	Set up new account and issue CCO	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
6	Closure of CCO before paid in full due to i) revoked to NIL or ii) written off	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
7	CCO debt secured	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
8A	CCO paid in full where debt has been secured	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
8B	CCO paid in full where debt was not secured	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
9	K&E Check fully completed & findings recorded	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
10	Appeal contribution paid in full	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]

Intentionally blank.

APPENDIX 1 TO SCHEDULE 2 (cont)

Table 2a: Solicitor's Fees and Professional Services

Type of Order / Writ	Year 1 (£ per case)	Year 2 (£ per case)	Year 3 (£ per case)	Year 4 (£ per case)	Option Year 5 (£ per case)	Option Year 6 (£ per case)
Charging Order	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Attachment of Earnings Order	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
High Court Writ	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Third Party Debt Order	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]

Table 2b: Court Fees and Enforcement Fees

Name	Price (£)
Applying to the court for an order to enforce the ICO or CCO - enforcement fee	[Redacted]
Applying to the court for an order to enforce the ICO or CCO - disbursement / court fee	[Redacted]
Charging Order - HM Land Registry search fee	[Redacted]
Charging Order - disbursement / court fee	[Redacted]
Charging Order - enforcement fee	[Redacted]
Charging Order - HM Land Registry registration charge - disbursement / court fee	[Redacted]
Applying for Attachment of Earnings - disbursement / court fee	[Redacted]
High Court Writ - Applying to instruct the HCEO - disbursement / court fee	[Redacted]
High Court Writ - Applying to instruct the HCEO - enforcement fee	[Redacted]
High Court Writ - HCEO Abortive Fee	[Redacted]

Applying for a Third Party Debt Order - disbursement/court fee	[Redacted]
Applying for a Third Party Debt Order - enforcement fee	[Redacted]
Agents fee for attending hearing for a Final Third Party Debt Order - disbursement / court fee (only payable if the interim TPDO is granted and the Court proceeds to a hearing)	[Redacted]

Table 3: Additional Legal Costs

Position / Level of Legal Advisor	Year 1 (£ per hour)	Year 2 (£ per hour)	Year 3 (£ per hour)	Year 4 (£ per hour)	Option Year 5 (£ per hour)	Option Year 6 (£ per hour)
Senior Solicitor/Legal Executive (Band A) - 8yrs+ post qualification experience	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Solicitor/Legal Executive (Band B) - 4yrs+ post qualification experience	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Junior Solicitor/Legal Executive (Band C)	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Trainee Solicitor/Paralegal (Band D)	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]

APPENDIX 2 TO SCHEDULE 2

COST BREAKDOWN

Table A

[illegible][illegible][illegible]

Telephony & Communications	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
HR Support	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
TUPE Costs	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Other Operating Costs	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Sub-Total Operating Costs	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]

Total Costs	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
-------------	------------	------------	------------	------------	------------	------------	------------

Total Contract Price (£)							[Redacted]
--------------------------	--	--	--	--	--	--	------------

Table B - Contract & Unit Prices

Total Contract Prices	Unit Price Year 1	Unit Price Year 2	Unit Price Year 3	Unit Price Year 4	Unit Price Year 5	Unit Price Year 6
Unit of Work Price - Set up new account and issue ICO collections letter	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Unit of Work Price - Closure of ICO before paid in full	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Unit of Work Price - ICO debt secured	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Unit of Work Price - ICO paid in full where debt has been secured	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Unit of Work Price - ICO paid in full where debt was not secured	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Unit of Work Price - Set up new account and issue CCO	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]

Unit of Work Price - Closure of CCO before paid in full	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Unit of Work Price - CCO debt secured	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Unit of Work Price - CCO paid in full where debt has been secured	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Unit of Work Price - CCO paid in full where debt was not secured	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Unit of Work Price - K&E Check fully completed & findings recorded	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Unit of Work Price - Appeal contribution paid in full	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]

APPENDIX 3 TO SCHEDULE 2
FLOW CHART OF UNITS OF WORK

[Redacted]

Intentionally blank.

APPENDIX 4 TO SCHEDULE 2
MINIMUM & MAXIMUM VIABILITY THRESHOLDS

TYPE	MINIMUM VIABILITY THRESHOLD	MAXIMUM VIABILITY THRESHOLD
Income Contribution Orders (ICO)	[Redacted]	[Redacted]
Capital Contribution Orders (CCO)	[Redacted]	[Redacted]
Capital & Equity Checks (K&E)	[Redacted]	[Redacted]

Intentionally blank.

SCHEDULE 1 – SPECIFICATION

**Crown Court Means Testing – Debt Collection and Enforcement Service
Specification**

1.	Introduction	4
2.	Background	4
3.	Objectives	4
4.	Definitions.....	5
5.	Overview of the Means Testing Scheme	6
6.	Scope	8
7.	IT Systems	17
8.	[Not used]	19
9.	The Supplier and Supplier’s Staff.....	19
10.	Customer Service and Complaints.....	20
11.	Legal Aid Means Test Review	22
	Appendix A – Process Flow Diagrams	23
	Appendix B – Capital & Equity Initial Sift Business Rules.....	25
	Appendix C – Business Rules for Re-Assessment of Pre Conviction Contributions.....	28

1. Introduction

- 1.1 The Ministry of Justice ("**MoJ**") and Legal Aid Agency ("**LAA**") acting on behalf of the Lord Chancellor (the "**Authority**") has appointed the Supplier to provide national Debt Collection and Enforcement Services from means-tested Defendants who are in receipt of legal aid in their Crown Court case. The Services cover all Crown Courts in England and Wales.
- 1.1.1 This Schedule 1 sets out the specification of requirements for which the Supplier is responsible including:
 - a) the collection and enforcement of legal aid contributions that require case management, collection, enforcement and, where appropriate, refunding of monies;
 - b) undertaking Capital and Equity Checks;
 - c) Administering Capital Contribution Orders.
- 1.1.2 Payments collected by the Supplier must be remitted to the Authority and the Enforcement Costs charged back to the Defendant whilst the Supplier ensures it keeps Defendants fully engaged throughout the lifetime of the debt.

2. Background

- 2.1 The LAA was created by the Legal Aid, Sentencing and Punishment of Offenders Act 2012, as an executive agency of the MoJ, and it runs the legal aid scheme in England and Wales. The LAA ensures that eligible individuals receive the legal advice, assistance and representation they need to deal with a wide range of problems. The LAA works in partnership with solicitors and not-for-profit organisations to ensure that these Services are provided to those individuals most in need.
- 2.2 Means testing Defendants' eligibility for legal aid was successfully introduced in the magistrates' courts in October 2006, realising substantial savings. Means testing was then implemented in the Crown Court in 2010.
- 2.3 The introduction of Crown Court Means Testing (CCMT) in 2010 underpinned the Government's commitment to the principle that those who can afford to pay for their defence should do so. It ensures that the best use is made of taxpayers' money and that limited resources can be utilised where most needed. The scheme ensures that Defendants appearing in Crown Court cases pay contributions from income or Capital or both towards their legal representation at a level appropriate to their financial circumstances.
- 2.4 Means testing in the criminal courts is governed by the Legal Aid, Sentencing and Punishment of Offenders Act 2012. Financial eligibility for criminal legal aid and relevant thresholds for criminal legal aid are outlined in the Criminal Legal Aid (Financial Resources) Regulations 2013. Contributions from Defendants for their criminal legal aid are governed by the Criminal Legal Aid (Contribution Orders) Regulations 2013 and the Criminal Legal Aid (Motor Vehicle Order) Regulations 2013.
- 2.5 The Government consulted upon the effectiveness of the CCMT scheme in October 2012 and issued its response to the consultation in March 2013¹. The proposals set out in the consultation paper sought to ensure that Defendants comply fully with the requirements of the scheme so that a comprehensive and accurate assessment of financial liability can be undertaken, as well as reinforcing existing measures to support more effective collection of contributions. As a result of this consultation process, a number of measures came into force 1st April 2013, as set out in the Regulations.
- 2.6 The Criminal Legal Aid (Motor Vehicle Orders) Regulations 2013 also came into force 30th July 2013. These regulations enhance the enforcement options available and grant the power to the Lord Chancellor to apply to the court for a vehicle clamping order and a vehicle sale order where an overdue amount is unpaid by an individual in receipt of criminal legal aid.
- 2.7 Defendants in the Crown Court in receipt of universal credit are currently passported and will receive criminal legal aid.

3. Objectives

- 3.1 The objective of this Contract is to ensure the Authority outsources quality and value for money Debt Collection and Enforcement Services to administer the Crown Court Means Testing scheme collection of criminal legal aid contributions from those who can afford to pay.
- 3.2 Throughout the Contract Period the Supplier must:
 - work strategically and collaboratively with the Authority to assist in achieving ongoing increase in performance and targets;
 - work innovatively in collaboration with the Authority in order to identify areas for improvement in the Services;
 - be able to adapt processes, procedures, underpinning IT infrastructure and MI to accommodate policy changes which will come into effect during the Contract Term.

¹ <https://consult.justice.gov.uk/digital-communications/crown-court-means-testing>

4. Definitions

- 4.1 Unless the context otherwise requires the following terms shall have the meanings given to them below. Other capitalised terms shall have the meanings given to them in the Terms & Conditions or Schedules in which they first appear.
- "Additional Payment"** means where an additional contribution is identified after the debt is finalised and leads to an increased amount having to be paid;
- "Appeal Case"** means all those activities associated with obtaining a Defendant's contributions towards the costs of an appeal;
- "Arrest Summons Number"** means the police reference number relating to a specific arrest;
- "Authority's Complaints Procedure"** means the Authority's complaints procedure as set out in [Complaints procedure - Legal Aid Agency - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/complaints-procedure-legal-aid-agency);
- "Business Rules"** means the parameters and rules that apply to the means testing scheme as set out in Appendices B and C;
- "Capital"** has the meaning set out in the Criminal Legal Aid (Contribution Orders) Regulations 2013 and includes savings, shares, stocks etc;
- "Capital and Equity Checks" or "K&E Checks"** means the Capital and Equity checks undertaken either by the Authority, the Supplier, or both the Authority and the Supplier in order to confirm the Defendant's available assets;
- "Capital Contribution(s)"** has the meaning set out in the Criminal Legal Aid (Contribution Orders) Regulations 2013;
- "Capital Contribution Order"** means a letter issued to the Defendant by either the Authority or by the Supplier confirming the amount of Capital Contribution that is required towards their Final Defence Costs;
- "Capital Evidence Sanction"** means a sanction which may be applied by the Authority to a Defendant where the Authority believes, on the evidence available to them, that the Defendant has undeclared or undervalued their Capital and Equity, and the Authority can withhold the [redacted] threshold to encourage the Defendant to provide further supporting evidence;
- "Case Reconciliation"** means the calculation undertaken to determine whether there is an outstanding debt to the Authority or a refund due to the Defendant;
- "CCMT"** means Crown Court Means Testing;
- "CCO"** means a Capital Contribution Order;
- "CCO Case"** means all those activities associated with making a CCO;
- "Change in Financial Circumstances"** means a change in the Defendant's financial circumstances;
- "CIFIC"** means Change in Financial Circumstances;
- "Collection System"** means an internet-based system set up by the Supplier to record Contributions Accounts, case notes, attachments and debt balances that can also be viewed on a read-only basis by licensed caseworkers at the Authority provided with user ID and password;
- "Complaints Log"** means the details of every Complaint received as recorded by the Supplier;
- "Contribution Account"** means an account set up by the Supplier to record individual case notes and case history, liability schedule and debt balances for a specific Defendant;
- "Contribution Order"** means either an Income Contribution Order (ICO) or a Capital Contribution Order (CCO);
- "Criminal Offence Data"** means personal data relating to criminal convictions and offences or related security measures as stipulated in the GDPR;
- "Crown Court Means Testing"** means the scheme whereby Defendant's financial means are assessed to determine whether that individual should pay a contribution towards their legally-aided defence costs from income or capital assets;
- "Debt Collection and Enforcement Services"** means the Services as described in this Specification;
- "Debt Management Recovery System"** means the system described under section 7 of this Schedule 1;
- "Debt Relief Order"** means a 12 month suspension of low priority debt (Authority is low priority debt) whilst other higher priority debts are paid. Obtained from the official receiver (an officer of the bankruptcy court) provided eligibility criteria is met, it places restrictions on the debtor;
- "Deed of Trust"** means the agreement that will be put in place between the Authority and the Supplier and/or a Sub-Contractor (or other third party) providing the Services under the Contract between the Authority and the Supplier. The purpose of the Deed of Trust is to ensure that any moneys seized or which comes into the possession custody or control of the Supplier and/or Sub-Contractor (or other third party) are held on trust for the Authority;
- "DRO"** means Debt Relief Order;
- "Equity"** means property or other capital asset value minus mortgage;
- "Final Completion Statement"** means a statement confirming the distribution of monies following a house sale, some of which may be payable to the Authority;
- "Final Contribution"** means the outstanding contribution required following conviction of the Defendant;
- "Final Contribution Notification Letter"** means the letter sent to the Defendant to notify them of the upcoming Final Contribution;
- "Final Creditor's Letter"** means the letter sent to Defendant to confirm that the debt balance is settled and paid in full;
- "FDC"** means the Final Defence Cost;
- "Final Defence Cost"** means the total costs of a case including both litigators' and advocates' fees;

"**Hardship Review**" means an Authority review of a Defendant's unusually high outgoings, the result of which could be to revise either their obligation to pay or the level of their contributions;

"**Hardship Route**" means a route available whereby Defendants facing financial difficulties can request their circumstances to be taken into account in the Means Assessment;

"**ICO**" means an Income Contribution Order;

"**ICO Case**" means all those activities associated with making an ICO;

"**IES**" means an Income Evidence Sanction;

"**Implementation Period**" means the period between the Commencement Date and Service Commencement Date;

"**Income Contribution Order**" means a letter issued by the Authority confirming the amount of pre-conviction monthly contribution required from the Defendant during court proceedings;

"**Income Evidence Sanction**" means a sanction applied by the Authority when the required supporting household income evidence is not provided to the Authority within 21 days of request. This sanction is set at either [redacted] or one twelfth of an applicant's disposable income, whichever is the higher;

"**Individual Voluntary Arrangement**" means an agreement with creditors (including the Supplier) whereby the Defendant agrees to pay all or part of their debts (including contributions);

"**INL**" means Individual Notification Letter;

"**Initial Notification Letter**" means an initial letter sent to the Defendant that introduces them to the debt collector company and notifies them of the amount due, how to contact the debt collection company and how to pay;

"**IVA**" means an Individual Voluntary Arrangement;

"**Judicial Proportion Order**" means an order that requires the Defendant to pay a proportion of the costs of representation in proceedings in the Crown Court, issued on the ground that it would be manifestly unreasonable to require the Defendant to pay the whole amount;

"**K&E Check**" means a check of the Defendant's and any partner's total household disposable Capital and Equity to determine the amount available above the [redacted] threshold and hence inform the level of contributions due under a Capital Contribution Order;

"**Means Assessment**" means the assessment of either the household income and deductions or the household Capital and Equity means of a Defendant and, where applicable, their partner;

"**Phase 5 case**" means a query sent by the Supplier to the Authority to establish when the Income Contribution Order (ICO) was sent to a specific Defendant and hence the effective date of the CIFIC;

"**Scheduler**" means a software component that initiates the triggering of data flow to the Supplier at specific times or on predefined schedules.

"**Sentence Order Date**" means either the date of acquittal or the date of sentencing in a convicted / part convicted case; and

"**SOD**" means the Sentence Order Date".

5. Overview of the Means Testing Scheme

5.1 As at the Service Commencement Date the means testing scheme in the Crown Court will apply to the delivery of the Services. The means testing scheme is summarised in Table A1.1 below. The process flow, detailed rules and timescales that apply the scheme are set out in Appendices A, B and C to this Schedule. Note that the means testing scheme will be revised in light of the results of the recent Means Testing Review. More detail about the likely impact of the Review is set out in Section 11 of this Specification.

Table A1.1 Means testing scheme for each type of case in the trial and conviction process

Type of Case	Scheme	Notes
Pre conviction – Criminal proceedings in the Crown Court – the Defendant is committed, sent, or transferred for trial	Income Contribution Order Case (ICO Case) An ICO is issued by the Authority, based on the Defendant's household disposable income. The contents of an ICO must comply with the requirements of Regulation 16 of the Criminal Legal Aid (Contribution Orders) Regulations 2013. Defendants who are liable for an income-based contribution will either pay for the life of the case or six months, whichever is the shortest. Defendants who pay on time, every month will only be required to make five payments. The contribution is 90% of household disposable income and the minimum monthly contribution will be is [Redacted]. This may also be limited to the maximum income contribution that is set depending on the type of case. The Regulations require ICO contributions to be paid within 28 calendar days Where Defendants fail to provide sufficient evidence to support the details provided in their legal aid application, an uplift in the sums due via an Income Evidence Sanction (IES) will be applied by Authority until the evidence is received – All Defendants who are acquitted will be refunded any monies paid with [Redacted] interest.	Pre-conviction Defendants will be means tested by the Authority under regulations (footnote 3) and they will either be: <ul style="list-style-type: none">• Passported² through scheme• Subject to income-based contribution³• Not liable for income-based contribution A Hardship Route is available for Defendants who wish to have their particular financial circumstances taken into account. A Change in Financial Circumstances (CIFIC) route also applies. These changes to liabilities can happen any time up until the conclusion of the court case and will mean that the Supplier will need to administer and issue notifications when there are changes and varying debt liabilities. These changes can take effect from the start of the case or from a date going forward.

² Defendants who are either under 18 or on a passporting benefit will not be required to contribute towards their legal aid costs, either during the case or at the end if convicted. Please refer to Regulation 9. (1), (2) and (3) of the Criminal Legal Aid (Contribution Orders) Regulations 2013.

³ Where the Defendant's disposable annual income exceeds [Redacted].

Type of Case	Scheme	Notes
Post conviction – Sentenced by Crown Court and found guilty or partially guilty	Capital Contribution Order Case (CCO Case) – A CCO is calculated based on Final Defence Costs (see below), balancing any monies paid to date and whether any outstanding costs remain. This is issued by the Supplier following completion of a K&E Check confirming available Capital and Equity assets in the Defendant's household, such checks are undertaken either by the Authority, the Supplier or both in specific prescribed circumstances as in the Business Rules in Appendix B. The contents of a CCO must comply with the requirements of Regulation 32 of the Criminal Legal Aid (Contribution Orders) Regulations 2013. The Regulations require CCO contributions to be paid within 28 calendar days When there is still a financial liability outstanding after conviction, then recovery of the balance will be made from Capital/Equity over the [Redacted] threshold. Recoveries of post-conviction debt can still be pursued against the pre conviction ICO if these are still outstanding at the point of conviction where there are Capital and Equity assets above [redacted] FDCs that are greater in value than crystallised ICOs where there is still a balance due that needs to be collected are required to be paid in 28 calendar days.	Post-conviction – Convicted or part-convicted Defendants will also be liable for case costs at the end of their case if they have any Capital/Equity once the allowance/threshold of [Redacted] has been deducted from the Defendant's total household assets and savings. A Hardship Route is available for Defendants who wish to have their particular financial circumstances taken into account. A Change in Financial Circumstances (CIFIC) route also applies. These changes to liabilities will mean that the Supplier will need to administer and issue notifications when there are changes and varying debt liabilities.
Appeals	Appeal Case contribution Defendants will be means assessed, with an additional allowance of [Redacted] deducted from their disposable income ⁴ . The total contribution will be a fixed fee depending on the outcome/type of appeal: <ul style="list-style-type: none"> Unsuccessful appeal against conviction [Redacted]; Outcome of appeal is unsuccessful, but sentence is reduced [Redacted]; Unsuccessful appeal against sentence [Redacted]; Successful appeal – zero contribution. 	If the Defendant is unsuccessful and they have failed the means test, the Defendant pays either [Redacted] or [Redacted] depending on type of appeal and outcome. This is collectable at the conclusion of the appeal.

- 5.2 At the post-conviction stage, the Supplier shall perform Capital and Equity Checks (K&E Checks) on particular Defendants (as set out in Appendix B) who have not yet had their Capital and Equity checked by the Authority at pre-trial. Checks should be undertaken upon conviction on those Defendants who have not covered their likely costs with an ICO but have declared more than [Redacted] Capital and Equity. As financial circumstances can change between the time of the legal aid application and the conviction/conclusion of the case at the Crown Court, the Supplier will - validate these cases to confirm whether the Defendant now has the means to contribute towards a post-conviction CCO. This also enables a check to be carried out in respect of any failure to declare Capital assets or a potential partner in the application for legal aid. This is an administrative process that will require the Supplier to utilise several commercially available products in order to validate the Capital and Equity declaration made by the applicant and to ensure addresses are up to date and thereby enable further evidence to be requested, where necessary. The validation services which the Supplier should have at its disposal include but are not limited to the Land Registry and commercial credit checks. Checks are not chargeable upon conviction on those Defendants who have already declared enough to cover their likely costs unless their Final Defence Costs subsequently exceed the amount available.
- 5.3 The Authority currently has a fortnightly data share in place with His Majesty's Prisons and Probation Service to obtain the most up to date prisoner locations and addresses which can be shared with the Supplier.
- 5.4 Where the convicted Defendant has told the Authority they have neither Capital nor Equity, the Authority will validate this on a sample basis. The Supplier will however be required to validate Capital and Equity means (K&E Check) for those convicted Defendants who have declared insufficient Capital and Equity above [Redacted] where the Final Defence Costs (FDC) are more than the available, declared Capital and Equity. Appendix B describes the Business Rules.
- 5.5 In accordance with the Criminal Legal Aid (Contribution Orders) Regulations 2013, the individual in receipt of criminal legal aid is also liable for any Enforcement Costs (see Schedule 2) incurred, and this amount is added to any amount payable by that individual. The Supplier must provide an appropriate and proportionate approach towards enforcement in accordance with regulations and Good Industry Practice.
- 5.6 The relevant regulations, underpinning the scope of the scheme, can be located here:
- The Criminal Legal Aid (Financial Resources) Regulations 2013 – <http://www.legislation.gov.uk/ukxi/2013/471/contents/made>
 - The Criminal Legal Aid (Contribution Orders) Regulations 2013 – <http://www.legislation.gov.uk/ukxi/2013/483/contents/made>
 - The Criminal Legal Aid (Motor Vehicle Orders) Regulations 2013 – <http://www.legislation.gov.uk/ukxi/2013/1686/contents/made>
- 5.7 For historical cases, the following Regulations will also still apply:
- The Criminal Defence Service (Contribution Orders) Regulations 2009 (as amended) – <http://www.legislation.gov.uk/ukxi/2009/3328/contents/made>
 - The Criminal Defence Service (Contribution Orders) (Amendment) Regulations 2010 – <http://www.legislation.gov.uk/ukxi/2010/142/contents/made>
- 5.8 Further information relating to the scope of legal aid and means testing can be located on the Justice website: <http://www.justice.gov.uk/legal-aid/assess-your-clients-eligibility/means-testing-in-the-courts>

⁴ This is to allow for any costs incurred in the magistrates' court, where Defendants have paid privately for representation

6. Scope

- 6.1 The Supplier will be required to manage Defendant accounts, log, monitor, trace and collect debt in relation to Defendants convicted in England and Wales. This includes administering and collecting a Defendant's contributions during the course of their case, and, once the case is concluded, either refunding over payments or pursuing further contributions. In the event that outstanding contributions remain unpaid, the Supplier is also responsible for pursuing the debt save where circumstances are such that the debt cannot be recovered and must be written off, as approved by the Authority.
- 6.2 The activities to be delivered are summarised below in Table A1.2. The process flow for these activities is set out in Appendix A to this Schedule, while the detailed Business Rules are set out in Appendices B and C. All standard correspondence and notification templates used to undertake these activities will need to be Approved by the Authority prior to use and the Authority may specify and provide a copy of template letters in order to optimise recovery rates.
- 6.3 The Supplier will be expected to ensure that all correspondence meets plain English standards. Wherever possible, the Supplier should also provide information in a format that would meet the Defendant's specific communication needs. In doing so, the Supplier should seek to ensure that a Defendant's individual preferences or needs are documented and stored on internal systems in order that future notices can be issued in the Defendant's preferred or required format.
- 6.4 The Supplier must ensure all dated copies of correspondence received from Defendants and replies or notifications sent out to Defendants by the Supplier are retained on its Collection System. In addition, all data feed receipts, Authority instructions, Supplier actions and decisions taken on setting up and managing the Defendant Account must be recorded and dated on the Collection System in order to enable the Authority to assure and audit the Supplier's performance, understand its decision making, and validate its achievement of KPIs.
- 6.5 The Authority requires the Supplier to ensure that the Services are accessible to, and understandable by Defendants whose language of choice is Welsh, in accordance with the Welsh Language Act 1993 (as amended) and Welsh Language (Wales) Measure 2011.
- 6.6 Some Defendants may also require communication in a foreign language. Any translation costs involved in contacting a Defendant in a foreign language would be considered an overhead for the Supplier, but the costings must be transparent to the Authority.
- 6.7 The Supplier must, and must procure that those Sub-Contractors who collect cash money from Defendants, pay those monies into a dedicated single Escrow bank account in accordance with the Deed of Trust for the sole purpose of receiving all Legal Aid contribution payments and enforcement costs from Defendants. A template of the Deed of Trust that the Supplier and any of its Sub-Contractors will be required to sign is set out in Schedule 19 (Deed of Trust). Bank statements from this account must reconcile with all collection and remittance financial reports provided to the Authority.

Table A1.2 Summary of activities comprised in the Services

Note that the references in Table A1.2 to Unit of Work References are to the Service Costs broken down by Unit of Work in Table 1 of Schedule 2 (Pricing and Payment). They are included to indicate which Unit of Work includes the relevant activity in this Table A1.2. Where there are multiple Unit of Work References against a particular activity, these are indicative only and the actual route that a case takes will determine which of the options of the Unit of Work References listed below will be applicable in the circumstances in question.

Pre-conviction	Post-conviction
Creation of a Defendant account within one (1) Working Day of receipt of the data file. Part of Unit of Work Ref. 1	Balance final case costs against any monies already collected in order to determine the Defendant's final liability. Final case balancing of ICOs is determined by whichever is the lowest of the following: 1. Maximum Income Contributions as per Legal Aid Means Test; 2. Income Contributions case cap; 3. FDC. Final case balancing of CCOs is determined by whichever is the lower of (i) FDC and (ii) available capital and equity over [Redacted]. This process is carried out on all post conviction cases. Part of Unit of Work Ref. 4 (4A or 4B) if post conviction ICO or Part of Unit of Work Ref 5 if a CCO. Part of Unit of Work Ref 9 if not an ICO case and no CCO subsequently issued
Initial introduction letter to all Defendants who are required to make income contributions, confirming payment options, to be sent within two (2) Working Days of Defendant account set up. Unit of Work Ref. 1	Refund Defendants who have either been acquitted or have overpaid through income contributions with [Redacted] interest within five (5) Working Days. If acquitted Unit of Work Ref. 2. If refunding because overpaid through income contributions when the case balancing action above upon receipt of FDCs is carried out then Part of Unit of Work Ref. 4 (4A or 4B).
Identify when multiple contributions are due from either married, cohabiting partners and/or scenarios where the Defendant has multiple cases that are live and collectable. These can be considered 'stacked' cases where collections are made and only one income contribution is collected from either the Defendant or their partner at a time. Part of Unit of Work Ref. 1.	Carry out a K&E Check as per Business Rules in Appendix B when conviction is confirmed in order to determine the Defendant's ability to pay the final balance owing from Capital and Equity assets within twenty (20) Working Days of the conclusion of the trial or the FDC being received. Quality criteria for KPI purposes are: 1. Total calculation of available Capital and Equity over [Redacted] is correctly calculated as at Sentence Order Date; and 2. Collection systems must show notes and outcomes of any required K&E checks and how values have been calculated. Unit of Work Ref. 9.
Collection of contributions from income. Part of Unit of Work Ref. 4 (4A or 4B).	As part of Capital and Equity check (K&E Check), request and chase further evidence where the Defendant has declared insufficient Capital and Equity to cover the full costs of the case. Available Capital and Equity is calculated by adding up all household assets and savings and adding this to Property net of outstanding mortgage, then deducting a [Redacted] allowance. Part of Unit of Work Ref. 9

<p>Remind /Chase Defendants where payment has not been received at least five (5) Working Days prior to the due date and, as applicable, chase payment no later than five (5) Working Days after the due date.</p> <p>Part of Unit of Work Ref. 2 or Unit of Work Ref. 4 (4A or 4B).</p>	<p>Issue contact letter within five (5) Working Days of conclusion of trial/sentence date and every three (3) months thereafter, to remind the Defendant that their final financial liability has not yet been confirmed and the Supplier will contact them again when final bills from solicitors and advocates have been received.</p> <p>This contact letter is sent out for all post conviction cases except where FDC is received before the conviction outcome is received.</p> <p>Part of Unit of Work Ref. 4 (4A or 4B) if post conviction ICO or</p>
--	---

Pre-conviction	Post-conviction
	Part of Unit of Work Ref 5 if a CCO. Part of Unit of Work Ref 9 if not an ICO case and no CCO subsequently issued
Recovery and allocation of outstanding debts. Part of Unit of Work Ref. 4 (4A or 4B).	Issue Capital Contribution Orders after final case balancing, upon receipt of Final Defence Costs or after completion of any required K&E checks whichever date is the later. Quality criteria for KPI purposes are: <ol style="list-style-type: none"> 1. Correct CCO template used and completed correctly in full; and 2. All Capital and Equity values and mortgage declared by defendant or found by the Supplier is listed and explains to the Defendant how available K&E above [Redacted] has been calculated; and 3. FDC value on CCO template. Unit of Work Ref. 5.
Tracing debtors and investigating means where appropriate. Part of Unit of Work Ref. 4 (4A or 4B).	Remind/chase Defendant where the final balance owing has not been received. Post Conviction ICOs - Part of Unit of Work Ref. 4 (4A or 4B). CCOs - Part of Unit of Work Ref. 8 (8A or 8B).
Recovery of outstanding payments from income using enforcement sanctions. Part of Unit of Work Ref. 4 (4A or 4B).	Recovery of outstanding payments post conviction using enforcement sanctions. Part of Unit of Work Ref. 8 (8A or 8B).
Issue notification when all pre conviction contributions paid. Unit of Work Ref. 4 (4A or 4B).	Issue notification when enforcement costs repaid and CCO paid in full. Unit of Work Ref. 8 (8A or 8B).
Deal with Defendant queries within five (5) Working Days. Part of Unit of Work Ref. 2 or Unit of Work Ref. 4 (4A or 4B).	If enforcement by way of a Charging Order is successful, manage the ongoing liability once secured, and transfer payment(s) made by the Defendant towards their Enforcement Costs back to the Authority when appropriate. Unit of Work Ref. 3 (if ICO) or Unit of Work Ref. 7 (if CCO) when debt secured at Interim stage.
Recalculate pre conviction liability and issue letters confirming any cases where liability reduced to [redacted] following advice from the Authority on an Income Contribution Order (ICO) within 5 Working Days. Unit of Work Ref. 2.	Make recommendations to the Authority for Approval to write off debts in line with Authority policy and processes for following categories of circumstances: <ul style="list-style-type: none"> • Defendant deceased; • Defendant untraceable; • uneconomic to pursue case; • Defendant assets repossessed; • negative Equity; • poor circumstances; • bankruptcy, IVA, DRO; • Defendant outside jurisdiction; • recovery is statute barred; • Charging Order administrative error; • unable to enforce. Unit of Work Ref. 2 for ICO or Unit of Work Ref. 6 for CCO.
Administer and recalculate varied debt liabilities notified by the Authority due to changes in circumstances (CIFC), Hardship Review, new information, Additional Payments, or Judicial Proportion Order and, where debt liabilities change, issue revised notifications of liability within five (5) Working Days of verification of information. Part of Unit of Work Ref. 2 or Unit of Work Ref. 4 (4A or 4B).	Supplier to review and reissue CCOs where CIFC apply, new evidence comes to light, or there is a variation due to hardship or Judicial Proportion Order within five (5) Working Days of verification of information. Part of Unit of Work Ref. 8 (8A or 8B) where there is ongoing CCO liability after reassessment. If CCO revoked and liability reduced to [Redacted] following reassessment – Unit of Work Ref. 6.
	Recalculate ICO post-conviction liability and issue letters confirming new income liability to [redacted] within 5 Working Days. Unit of Work Ref. 2. Where a post conviction ICO is reassessed to Nil – any payments made would be transferred to the CCO – it would not be refunded with interest, unless there was no CCO payable.
	Deal with Defendant queries within five (5) Working Days. Part of Unit of Work Ref. 3 or Unit of Work Ref. 4 (4A or 4B) if post conviction ICO or Part of Unit of Work Ref.6, 7 or 8 (8A or 8B) if a CCO.
	Unsuccessful Appeal against Sentence [redacted] contribution or Unsuccessful Appeal against Conviction [Redacted] contribution. Issue contribution collection letters and collect debt. Unit of Work Ref.10.

6.8 **Creation of Defendant account** - In order to start the contribution collection process, the Supplier will receive a data file from the Authority via secure transfer. A new collection account will be set up, within one (1) Working Day, based on the data provided.

6.9 Each account/Defendant profile that is created will include the following data:

- Authority unique ID – i.e. Legal Aid Means Assessment & Appeals Tool (MAAT) reference number (for each criminal case);*
- Defendant name, date of birth, address, national insurance number;*
- Defendant contact details (including address, postcode, telephone number, mobile number, email);*
- Defendant banking and payment details;
- type of offence;*
- Defendant contribution amounts and changes to contribution amounts following reviews of financial circumstances; *
- Defendant declared Capital and Equity listed assets and values;*
- Outcome of court case (acquittal, conviction or part conviction);*

- Sentence Order Date;*
- history of any payments made or missed;
- history of enforcement/recovery actions and costs;
- history of any amendments to a Defendant's contribution level;
- history on interest applied;
- Outcome of Supplier K&E Check and list of assets and values and calculations;
- post-conviction debt;
- Final Defence Costs (FDC)*;
- final balance*;
- write-offs;
- refunds and interest payments applied to refunds;
- history of acquittal or conviction;
- correspondence history;
- outbound and inbound call history including any SMS texts; and
- any other agent contact i.e. face to face or special campaigns.

* This data will be supplied by the Authority as part of the data file.

6.10 Updated data will be transferred from the Authority to the Supplier if the Defendant's details change after the information was originally passed over. This could be due to:

- change in contact details including address changes. The Supplier must also inform the Authority if they receive notification of any address change;
- change in the Defendant's financial circumstances or other reassessment reason;
- a Hardship Review has resulted in a revised monthly contribution level, additional evidence has been provided, or the K&E Check has been completed;
- the Equity/Capital level has been verified;
- the Defendant has provided additional evidence as requested, and the temporary sanction has been removed.

6.11 For the purposes of UK GDPR and the Data Protection Act 2018 it should be considered that the data being transferred is Criminal Offence Data.

6.12 **Collection of contributions from income** – The contribution details will be supplied as part of the original data file from the Authority. Contributions should be collected for the life of the case, or six (6) months, whichever is the lesser. Contributions will also be subject to a case type average cost cap, the details of which will be provided by the Authority to the Supplier. Defendants who make their first five (5) payments each month on or before the due date will be exempt from the sixth and final payment⁵. In addition, there will be an option for the Defendant to make a one-off payment of five (5) times the monthly contribution, prior to the date that the first monthly payment is due.

6.13 The Defendant may be subject to an Income Evidence Sanction (IES) if they have failed, without reasonable cause, to provide documentary evidence of income within 21 (fourteen (14) and further a further seven (7)) days. It may be judged that the Defendant is liable to pay six (6) contributions of [redacted] or one twelfth of the Defendant's disposable annual income (if the Authority is able to determine this without documentary evidence provided), whichever is the highest. Details of such instances will be passed on to the Supplier by the Authority.

6.14 In accordance with Regulation 23 of the Criminal Legal Aid (Contribution Orders) Regulations 2013, the director of Legal Aid casework may also determine that the Defendant is liable to make an Additional Payment following a reassessment of the Defendant's income.

6.15 The Defendant will pay either their full monthly pre-conviction contribution; make a partial payment, overpayment or nil payment. The amount paid should be balanced against their outstanding balance and the Defendant advised of the same, including any arrears. The balance amount may change as a result.

6.16 The Defendant will make the monthly contributions whilst the case/trial is in progress or until the maximum number of income contributions has been reached. There will be instances where Defendants have more than one case in the system at the same time or could be asked to make an additional contribution.

6.17 Defendants who have multiple cases running may have to pay a contribution for each of the cases in which they have been granted a representation order, although payments will only be taken in respect of one case at a time. Monthly contributions should, therefore, still be collected from an acquitted Defendant if they are still receiving legally aided representation for other Crown Court cases (that are running concurrently and have not yet concluded).

For example:

Defendant is receiving legal aid for two cases – Case A and B

Defendant is paying [Redacted] per month in contributions

Case A concludes and the Defendant is acquitted.

Case B has not concluded.

In these circumstances:

- Defendant is not liable for any defence costs for Case A;
- previous contributions received are not automatically refunded;
- previous contributions are rolled over for consideration against Case B costs;
- Defendant continues to pay [Redacted] monthly contribution either until the six-month cap is reached or conclusion of Case B.

6.18 The Supplier will be responsible for setting up a range of payment options, managing the accounts, monitoring the success or payment methods and sanctions, and collecting the monthly payments through the Defendant's preferred payment mechanism.

6.19 To maximise recovery rates, the Defendant should be provided with a variety of payment methods in order to make the payment of contributions as simple and convenient as possible.

This will include, but not be limited to, paying through the following channels:

- direct debit;
- standing Order;
- debit and credit card payments by telephone;
- cheque;

⁵ Please refer to paragraph 14 of the Criminal Legal Aid (Contribution Orders) Regulations 2013.

- giro;
- paypoint card;
- online payments;⁶
- mobile app.

6.20 **Initial introduction letter** - Upon setting up the Defendant account, the Supplier will send an initial contact letter to the Defendant. The letter will be sent within two (2) Working Days of creating the Defendant account and should as a minimum include:

- MAAT reference number;
- the Supplier's contact details;
- payment due date, including date first payment due;
- expected monthly contribution amount;
- total expected payment;
- details of the optional one-off payment of [Redacted] instalments;
- hardship details (options for the Defendant to challenge the amount the Defendant is expected to pay as a monthly contribution);
- reminder of the Defendant's obligation to notify of any change in contact details and financial circumstances;
- available payment methods;
- details of consequences arising in relation to any overdue payment;
- possible enforcement actions and any potential repercussions for non-payment or non-compliance;
- reminder that the Defendant is liable for any Enforcement Costs incurred;
- confirmation of preferred communication method;
- inclusion of regulations which stipulate Authority to act on behalf of Director of Legal Aid (Sec 3 Legal Aid, Sentencing and Punishment of Offenders Act 2012);
- notification that the Defendant's liability may increase post-conviction should further litigator and advocate bills be received;
- signposting to debt advice agency.

6.21 **Chasing/reminding Defendants** - The responsibility will be on the Defendant to contact the Supplier to inform them of their preferred payment date and method if they have not already done so.

Defendants who do not comply should be contacted within a maximum of five (5) Working Days of a missed payment and asked to provide the following:

- preferred method of payment;
- preferred payment date (e.g. 1st of the month);
- banking details (account number, name, sort code) if they choose to pay by direct debit;
- credit card information;
- preferred communication method;
- notification that the Defendant's liability may increase post-conviction should further litigator and advocate bills be received.

6.22 To ensure that Defendants are aware of how much they are expected to contribute, when they are expected to pay, and the consequences of non-payment, a range of tailored messages, reminders and chase letters should be made available.

This may include communication to Defendants through one of the following preferred methods:

- SMS text;
- telephone;
- text-to-voice message;
- letter;
- face-to-face engagement.

6.23 The Defendant's preferred communication method should be ascertained and stored on internal systems for future reference. This may include providing communication in the Welsh language, foreign languages, or making reasonable adjustments for Defendants with disabilities (e.g. providing information in large font).

6.24 A maximum of five (5) Working Days before a contribution is due to be paid, the Supplier will send a reminder, using a suitable communication channel, to the Defendant. As a minimum, this will include:

- date the payment is due;
- amount due to be paid;
- any supporting information needed to make the payment – e.g. MAAT Ref No.;
- information on possible sanctions for non-payment;
- contact and payment details;
- notification that the Defendant's liability may increase post-conviction should further litigator and advocate bills be received.

6.25 **Recovery and allocation of outstanding debts** - Accounts should be updated to monitor the contributions made by Defendants, and their case balanced accordingly. This includes recording:

- date of payment;
- amount of payment;
- method of payment;
- total contributions made to date (specifying funds which have cleared and are pending clearance);
- update an ongoing payment history;
- contribution balance.

There should also be an ability to provide a Defendant with a 'statement', either on a regular basis or on demand, of their payments made to date. This includes an end of payment statement.

6.26 Balancing the contributions made by a Defendant for active/open case(s) against the expected monthly contribution would result in:

- Defendant being in credit if they have overpaid;
- Defendant being in debit if they have either underpaid or missed payments;
- Defendant having zero balance if they have paid exactly the monthly contribution level or upfront payment;
- applying the cost for any enforcement actions taken (due to non-payment) onto the Defendant's balance.

The payment balance will then define the amount of the next monthly payment due from the Defendant and may act as a trigger for either supported or enforced recovery.

⁶ Should the Supplier use payment methods which can be reversed by the client (e.g. World Pay), the onus will be on the Supplier to reimburse the Authority.

- 6.27 There is also a requirement to enable a Defendant's revised contribution level to be backdated, for example following a Hardship Review by the Authority, and therefore to recalculate a current balance. This will result in all monthly contributions being set at the new recalculated level. Some reassessments can also be back dated but change in financial circumstances will normally operate going forward. See the reassessment rules in Appendix C of this Specification.
- 6.28 If the Defendant pays an upfront contribution before the first payment date, or pays all sums due, the Supplier will send a notification to the Defendant informing them that no further monthly contributions will be required through the course of the case. The notification will need to confirm that a Capital or Equity contribution might still be required if the Defendant is convicted and has Capital or Equity above the threshold and their FDC are greater than the amount already paid to date.
- 6.29 If the Defendant fails to make a payment on the designated date, the Supplier will record the non-payment and a second reminder will be issued giving the Defendant the opportunity to make the payment or to contact the Supplier for advice. The second reminder will be sent [Redacted] prior to any payment due date and will also contain information on how to make an application for a Hardship Review, to ensure that the Defendant is aware of the support available to them.
- 6.30 **Tracing debtors where appropriate** – If it becomes known, e.g. a letter is returned by the post office, that the Defendant has left the address that is held for them the Supplier will undertake activities to trace them. This is likely to include, but is not limited to, electoral roll checks, tracing tools and any publicly available HMPPS prisoner data where such data is not provided by the Authority.
- 6.31 **Issue notification when all contributions made/costs repaid** - The Supplier must be able to automatically suspend contributions and reminder notices at the conclusion of the case, in the event that the Defendant does not have any outstanding Contribution Orders in other proceedings running concurrently.
- 6.32 In order to stop collecting/expecting contributions from Defendants the Supplier needs to be made aware that the trial has concluded. This information will be included in the daily data file:

Trials

- MAAT reference number;
- Defendant's name (forename and surname);
- Defendant's date of birth;
- address;
- postcode;
- case number;
- arrest summons number ("ASN");
- Sentence Order Date;
- bench warrant issued? Yes/No
- convicted? – Yes/No
- imprisoned – Yes/No

Appeals to the Crown Court

The appeal type field is mandatory for all appeals. Data will be required when the appeal contains one of the following values:

- appeal against conviction;
- appeal against sentence.

The following data items are required for appeals:

- MAAT Ref No.;
- Defendant's name (Forename and Surname);
- Defendant's date of birth;
- address;
- postcode;
- case number;
- ASN;
- Sentence Order Date;
- dismissed? – Yes/No/Partially;
- imprisoned – Yes/No;
- appeal type.

- 6.33 The case verdict data file will be sent to the Supplier via a secure transfer mechanism on a daily basis.
- 6.34 The provision of the Sentence Order Date (SOD) will inform the Supplier to suspend the collection of any further payments, or the distribution of any payment reminders. However, in these instances where the Defendant is involved in multiple cases, contributions will continue to be required for the remaining cases. The Supplier will also need to calculate that the correct number of contributions have been collected.
- 6.35 Supplier will be informed of the trial ruling /court case outcome (Outcome). At this point the Defendant account will need to be updated to determine whether the Defendant has been convicted of one or more offences or the Defendant has been acquitted. From this, the Supplier can establish whether the Defendant is:
- eligible for a refund (i.e. contributions exceed defence costs or Defendant has been acquitted);
 - still has a financial liability (i.e. arrears exceed contributions made);
 - did/did not require enforcement activities/enforced compliance to recover any missed payments.
- 6.36 Defendants who still have a liability will have this added to any balance of case costs, which will then be compared against their Capital assets, in order to, define outstanding debt. Any arrears should continue to be pursued.
- 6.37 **Determination of final liability** – If a Defendant either pleads guilty or is found guilty on any charge within their case, they may be liable to meet their legal aid costs. This includes Defendants who had multiple charges and were found guilty on some charges and not guilty on other charges.
- 6.38 The FDC data will be sent to the Supplier on a daily basis. The file will contain records of all Defendants who have had a FDC calculated that day, and will contain the following data:
- Defendant's name;
 - case number;

- FDC amount;
- ASN.

6.39 This file will exclude acquitted Defendants, as they will have a nil financial liability.

6.40 However, the Authority retains the right to instruct the Supplier to enforce on partial liabilities.⁷

6.41 It is expected that the Supplier will already have been updated with the verdict/ruling of the case. When it receives the FDC for a Defendant, therefore, it will already know whether the Defendant was acquitted or found guilty and whether the FDC needs to be used for Case Reconciliation. There can be a delay of up to six (6) months between the end of the case and notification of FDC. In exceptional circumstances, this could extend beyond that period.

6.42 The Supplier will use the following information to determine the balance on the Defendant's account:

[Redacted]

6.43 If this calculation results in the Defendant being "in credit", the Defendant will be refunded the credit amount plus 2% interest, minus any recovery costs incurred, and the Defendant's account will be closed, however, the Supplier must have the ability to re-open Contribution Accounts to take into account further costs relating to the case:

[Redacted]

6.44 Interest may be added to any debt owed to the Authority by the Defendant. This would be calculated after:

- all cases are concluded;
- FDC for all convicted cases are received;
- final liability is calculated (i.e. contribution vs. costs);
- final debt is calculated (i.e. liability vs. Capital and/or Equity);
- a Defendant requires a refund.

Where it is determined that interest applies, interest will start to be calculated from a date as agreed between the Supplier and the Authority. Interest is calculated on the contribution amount only, and not on any associated Enforcement Costs. For debts passed for recovery by enforcement, the interest rate will be 6% compound per annum, with annual rests.

6.45 **Refunding Defendants** - Once the case has been closed, reconciled and a final balance established, Defendants who are acquitted will have their contributions refunded (with interest but less any recovery costs incurred) unless the judge rules that the Defendant is still liable for all, or a portion of, their costs due to their conduct. This refund must be sent within five (5) Working Days of notice from the Authority that a Defendant has been acquitted.

When the Outcome data is updated and the contribution collection stopped, the total amount that the Defendant has contributed to that point will be calculated.

6.46 If the Defendant's account, during the course of their trial, has incurred additional costs at the enforced compliance stage, these will be deducted from the final refund amount. Additional costs can include things such as bank charges paid by the Supplier for the non-payment of direct debits etc. Interest will be added to the total contributions the Defendant will be refunded, i.e. total contribution amount plus interest earned less any Enforcement Costs incurred.

6.47 As part of the refund process all cases will need authorisation from the Authority before a refund is issued.

6.48 As a minimum, refunds should be made available through the following channels:

- cheque;
- BACS transfer;
- debit / credit cards.

6.49 It should be recorded where a Defendant receives and banks any outstanding refund from the Authority. This includes closing the Defendant's contribution case on the Collection System.

6.50 Upon the conclusion of the Defendant's case in the Crown Court, the Authority will provide a status update to the Supplier by transmitting one data file with the case outcome and, once the barrister and solicitor claims have been paid, another separate data file containing the FDC. The Supplier will reconcile this data file against their system to determine the Defendant's final liability. Where the Defendant's payments have exceeded the cost of the case or the Defendant has been found not guilty, a refund including interest will be due.

6.51 Where refunds are due, the Supplier will off-set the value of any refund against monies collected from Defendants' contributions and provide a case breakdown to the Authority to support the invoice.

6.52 Where the value of any refund due exceeds those monies collected from Defendant's contributions, and the value of the refund is such that it would be unreasonable to expect the Supplier to make payment of such sums, the Supplier will submit an invoice to the Authority for value of the refund.

6.53 For refunds and overpayments, the interest rate will be **[Redacted]** compound per annum, with rests annually. Where applicable, the cost of any enforcement action taken against the Defendant will be deducted from the refund value.

6.54 Interest on refunds should be calculated at the point of receipt of the final monthly payment. If there has been a break in the payment cycle, and interest on the debt has been notified by the Supplier, interest will be calculated on the debt period first, and that figure will be deducted from any refund. Only then will a calculation be made to establish the amount of the refund due.

6.55 After processing the refund, the Defendant's account will be updated to show a zero balance and the account will be closed.

6.56 Exceptions – multiple cases

Defendants who have multiple cases will not receive a refund until all their cases have concluded:

- if the Defendant is acquitted on all cases they will receive a refund (minus any recovery costs incurred) plus interest;
- if the Defendant is acquitted on some cases they may receive a partial refund – dependant on case balancing;
- if the Defendant is acquitted on some cases their account may be in debt – dependant on case balancing.

⁷ Partial liabilities are where one element (either advocate or litigator bill) has been submitted but the other remains outstanding over 9 months from Sentence Order Date.

6.57 Exceptions – judicial apportionment on costs

- Defendants who are partially convicted⁸ may also be liable to partially contribute toward the cost of their defence if the judge recommends it. In this event, the ruling will be passed to the Supplier who will need to update the Defendant's account. The impact of a judicial proportion order is that the maximum a Defendant can be liable for is the percentage of the Final Defence Costs that the Judge deems appropriate.

6.58 As a minimum, K&E Checks will need to be done within twenty (20) Working Days of data file receipt of both convicted/partially convicted status or FDC.

6.59 The Supplier will not need to conduct K&E Checks on cases:

- where the declared Capital and Equity exceeds the income contribution cap;
- where the declared Capital and Equity covers the crystallised FDC;
- where the declared Capital and Equity is under [redacted];
- where the status is "verified" by the Authority.

6.60 Checks will be undertaken where:

- where an applicant's declared Capital and Equity is more than [Redacted] but does not exceed the income contribution cap. This check will be done at the point the Supplier receives the outcome of the case and where the outcome is confirmed as convicted or partially convicted;
- where the outcome is confirmed as convicted or partially convicted and the FDC's exceed the income contribution cap which results in the applicant's declared Capital and Equity no longer being sufficient to cover the FDC's.

6.61 Appendix B provides specific instructions in relation to the Business Rules that govern the checks required by the Supplier.

6.62 Once the final Capital and Equity means have been identified, and calculations recorded and explained, then the Supplier will add this to the Collection System and the confirmed amount can be used to calculate the outstanding debt/liability and to issue CCO notifications.

6.63 The amount of any outstanding contribution for those Defendants that exceed the Equity and Capital threshold is dependent upon how much they exceed the threshold by.

6.64 To accurately calculate the outstanding debt that the Defendant is liable for, the liability needs to be compared against the amount of Capital and/or Equity that the Defendant has above their allowable threshold. For example:

convicted Defendant has FDC of [Redacted]
Defendant has Capital of [Redacted]
Defendant has mortgage of [Redacted]
Defendant Equity in Capital is [Redacted]
Defendant has Capital allowance/threshold of [Redacted]
Final Capital and Equity is [Redacted]
CCO is [Redacted]

6.65 **Exceptions – Capital Evidence Sanction**

- The applicable Capital and Equity threshold is a combined [Redacted]. If a Defendant has failed to provide their Capital evidence within twenty one (21) days following their conviction, their allowable threshold of [Redacted] may be removed and the Supplier is entitled to recover any assets it was able to locate.
- Where it is proved that Defendants have falsely represented their Capital or Equity position, full details should be reported to the Authority's assurance team.
- Where there is a change in circumstances or new evidence comes to light, the Supplier will be required to review, reassess and reissue the CCO. If the value of the debt is reduced, notification to the Authority should be provided.
- Where the Supplier can evidence Capital and Equity from the information declared by the Defendant, or from K&E Checks as per Appendix B, they should continue to use this information to calculate the CCO and the final balance. The Authority may advise the Supplier to use a different or higher Capital and Equity means assessment figure, as part of the Authority's approach to Capital Evidence Sanctions, where the Authority believes, on the evidence available to them, that the Defendant has undeclared or undervalued their Capital and Equity, and to encourage the Defendant to provide further supporting evidence.
- Where a Defendant fails, without reasonable excuse, to comply with a request for information or documentary evidence in relation to Capital and Equity, the Authority has reasonable grounds to believe that the Defendant has Capital of an amount or value equal to, or in excess of, the recoverable costs of representation, the Authority can remove the [Redacted] threshold and request the full amount of the costs of representation less any monies already paid under an ICO.
- In any scenario where the Defendant's liability over a certain financial threshold as stipulated by the Authority is reduced or ceases, the Supplier should notify the Authority by email in advance. Once the FDCs are received, the Defendant will need to be contacted and informed of their outstanding debt and that interest will be applied to the debt on a monthly basis. This notification must be sent within five (5) Working Days of receipt of the FDC from the Authority. The Defendant must be encouraged to make a one-off payment but a facility should be in place to enable an instalment arrangement to be agreed so that the Defendant can pay the debt over an agreed period of time, or use a combination of both options i.e. settle an agreed amount, with the balance payable in instalments.

6.66 **Collection of final balance, including notification of final balance** - Those Defendants who at the conclusion of a case have been convicted; have Capital or Equity above the threshold; and have an outstanding debt, will be expected to pay the balance of the cost of their case. Once the final amount has been calculated the Defendant will need to be informed of:

- breakdown of how the Final Contribution has been calculated;
- the amount of the debt;
- payment options available;
- Authority's enforcement and recovery rights in the event of non-payment;
- level of compound interest that may be added on a monthly basis;
- ability to appeal against Final Contribution (i.e. appeal against level of Capital required to pay);
- contact details of the Supplier;
- a notification that liability may increase if further bills are received.

⁸ Where the Defendant is charged with more than one offence, and convicted of one or more, but not all.

- 6.67 **Notifications to be sent whilst awaiting defence costs** – After the sentence order and conviction any Defendant that still has a potential outstanding liability will require a reminder letter at this stage and every three (3) months thereafter until the FDCs have been received from solicitor and/or advocates and final financial liability can be calculated. The Defendant will also need to be notified that if they have any Capital and Equity above [Redacted] any outstanding liability may be recovered from their Capital and Equity.
- 6.68 Defendants who are convicted/part convicted under the K&E scheme (i.e. they do not have any liability under the ICO scheme because they did not have sufficient income) who have declared K&E above [redacted] will need to be reminded by letter within five (5) days of the trial ruling that the Authority is now awaiting the FDC which may take another six (6) months and they may have to make a contribution from their Capital and Equity once the Authority knows the final costs of their legal aid.
- 6.69 If the Defendant can demonstrate that they can only afford to pay monthly instalments, the Collection System will calculate the amount due based on the Defendant clearing the debt over an agreed period of time at an agreed rate. The Supplier can agree to instalment plans which would enable the liability including any interest accrued to be cleared within [Redacted], and will refer to the Authority for the possibility to agree extended payment plans beyond 12 months.
- 6.70 Similarly, to the collection of contributions during the course of the case, the Defendant will have a range of payment channels available to them, including:
- direct debit;
 - standing order;
 - debit and credit card payments by telephone;
 - cheque;
 - giro;
 - paypoint card;
 - online payments;
 - mobile app.
- 6.71 **Remind and chase Defendants where final balance not received** - The Defendant will receive notifications and reminders through one of the following preferred methods:
- SMS text;
 - email;
 - text to voice message;
 - letter;
 - telephone;
 - face-to-face engagement.
- 6.72 **Existing Debt** – The Supplier must demonstrate innovative and proactive expertise in reducing and collecting the existing debt accrued to date.
- 6.73 **Handling Defendant enquiries** – The Supplier must provide facilities to respond to Defendant's enquiries regarding their account. If these queries are challenging the contribution level or Capital determination they may need to be referred back to the Authority. Correspondence must be responded to within five (5) Working Days from receipt by the Supplier.
- 6.74 If the Defendant fails to respond, or does not make a payment, an initial chasing/reminder notification will be sent to them informing them of their responsibility to pay and the enforcement routes open to the Authority/Supplier for non-payment. This could take the form of a letter before action when enforcement is considered a practical, commercial option.
- 6.75 Any enforcement activity undertaken by the Supplier will take place in the County Court and/or the High Court.

Enforcement

- 6.76 **Application of enforcement sanctions (contributions and final balance)** – All applications issued to the Courts should name the applicant as the "[Service provider name] on behalf of the Lord Chancellor and Legal Aid Agency". It is expected that Defendants will fall into the following categories when recovering monies:
- voluntary – pay with little or no intervention;
 - supported – need some assistance before paying;
 - enforced – require the use of enforcement sanctions before payment is received.
- 6.77 The emphasis should be on targeting the right activities at the right stage to optimise recoveries in the most cost-effective manner.

Table A1.3 Summary of expected activities during the cost recovery process

Stage of Compliance	Pre Conviction	Post Conviction
Voluntary	Initial Notification Letter Initial reminder [Redacted] Days before payment due)	Final Contribution Notification Letter Initial reminder ([Redacted] Days before payment due) Need to issue reminder letter at Sentence Order Date and every three (3) months thereafter, to remind that their financial liability has not yet been received.
Supported	Reminder letter ([Redacted] Days after payment due date) Telephone call SMS Text message E-mail Voice to text message Advice regarding Hardship Route	Reminder letter ([Redacted] Days after payment due date) Telephone call SMS Text message E-mail Voice to text message Advice regarding appeal route
Enforced	Attachment of Earnings Order Distress Warrant Warrant of Execution Motor Vehicle Clamping Order or Motor Vehicle Sales Order Face-to-face engagement	Attachment of Earnings Order Charging Order, which could extend to obtaining an Order for Sale where Authority agrees is appropriate Third Party Debt Order Removal of Capital threshold – sanction for non-compliance with evidence provision Motor Vehicle Clamping Order or Motor Vehicle Sales Order

Table A1.4 Sanctions available in the enforced compliance state

Pre- Conviction	Post-Conviction
Attachment of Earnings Order	Third Party Debt Order
Distress Warrant/Warrants of Execution	Charging Order, including obtaining an Order for Sale
Motor Vehicle Clamping Order and Motor Vehicle Sales Order	Attachment of Earnings Order
	Motor Vehicle Clamping Order and Motor Vehicle Sales Order
	[Redacted] interest on money owed
	High Court Order

- 6.78 The Supplier should have the necessary personnel and legal expertise to ensure the official undertaking of all enforcement options. They will also need to consider if incurring additional costs for any type enforcement will be cost effective and result in the successful collection of outstanding debt.
- 6.79 If any Enforcement Costs are incurred while trying to collect the contribution, during the enforced compliance stage, they will need to be recorded as a Defendant cost. The amount incurred in relation to Enforcement Costs will be added to the Defendant's account and will increase the total outstanding payment balance. These additional charges are non-refundable in the event of a not guilty verdict or the case being abandoned. If however, incorrect or unreasonable Enforcement Costs are incurred by the Supplier then this will be charged back to the Supplier.
- 6.80 **Tracing debtors** – If it becomes known, e.g. a letter is returned by the post office, that the Defendant has left the address that is held for them the Supplier will undertake activities to trace them. This is likely to include, but is not restricted to, electoral roll checks and tracing tools.
- 6.81 **Manage the on-going charge if successfully applied to a property** - If no payment is made, the Supplier will check the Collection System to see if the Defendant has any Equity. If the Defendant has more [Redacted] in Equity, a land charge could be applied to the Defendant's property and the Defendant will be informed. Costs and land registry fees will be added to the debt and interest will accrue. Once the land charge is lodged in on behalf of the Authority, the debt should be managed by the Supplier from that point forward. The Supplier should continue to encourage the balance to be reduced. The Supplier should consider Orders for Sale where there are additional properties that are not the family home.
- 6.82 **Motor Vehicle Clamping Order and Motor Vehicle Sales Order** – The Criminal Legal Aid (Motor Vehicle Order) Regulations 2013 came into force [Redacted]. As part of the enforcement activities available to the Authority, these regulations provide the ability for the Authority to apply to the magistrate's court for a Motor Vehicle Clamping Order and a Motor Vehicle Sales Order against monies owed by a Defendant. Applicable charges for the undertaking of these activities are outlined in Schedule 1 of the Regulations. Operational guidance in relation to Motor Vehicle Clamping Orders and Motor Vehicle Sales Orders was issued by the Authority 30th July 2013:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/366552/motor-vehicle-order-scheme-guidance.pdf
- 6.83 **Assessment in respect of the Authority's write off policy** – There may be instances when after undertaking an assessment the Supplier concludes that the effort and/or expense involved in recovering the debt exceeds the probable amount that will be recovered. The Supplier will be able to recommend that the Authority writes off debts within the Authority's parameters. It will be for the Authority to agree based upon the evidence provided by the Supplier. Agreed debts for write-off will then need to be reflected in individual case records and in Supplier's financial accounts.

Table A1.5 Debt write-off

Reason and Code	Description	Evidence
01 - Debtor whereabouts unknown	The debtor cannot be traced.	Credit report that confirms client cannot be located, and at least three (3) trace attempts made over two (2) years in case of the Defendant's re-emergence on credit reports under a new address plus a final Authority credit check on Equifax at time of write-off.
02 – Uneconomic	Further recovery action is not cost-effective i.e. it is likely the cost incurred will not be recovered and debt is below <i>de minimis</i> threshold of [Redacted] for crime.	Documentation and review of credit reports to confirm the debtor does not have any assets or income to re-pay the debt. Debt less than [Redacted]
03 - Poor circumstances	Debtor does not have the capacity to repay.	Vulnerability factors – e.g terminal illness, mental health issues compromising ability to pay, recovery of payments unlikely to be possible as a consequence. Alongside vulnerability above, evidence that collection of debt would have disproportionate impact and be unreasonable e.g long delays to issuing ICO or CCO or long delays to issuing revised debt after previous closure, the Authority's errors or the Authority's misinformation /mis-advice. Personal budget form has been completed and evidence of change or continuing poor financial circumstances has been provided from credit checks, Land Registry (and possibly HMRC data) [Redacted] years post release from prison or post-conviction for the debtor to improve any financial circumstances before accepting they were unlikely to regain their pre conviction financial ability to pay.
04 - Debtor deceased	The debtor deceased and no recovery from estate.	Copy of death certificate or probate and statement from the executor/administrator that there are no assets to distribute after two (2) reminders.
5a - Debtor bankrupt 5b IVA or post payment agreement period expiring 5c DRO post payment period satisfied and expired	Bankruptcy or insolvency status.	Copy from the insolvency register confirming the date of hearing and bankruptcy/IVA or DRO number and confirmation that debt is listed. <u>Bankruptcy Order</u> , Final Creditor's Letter or letter from the official received confirming a proof of debt has been submitted, debt is listed as part of order and that there is no or partial dividend for unsecured creditors. <u>IVA/DRO</u> Confirmation that IVA or DRO has now come to end of agreement period ([Redacted]). Personal budget form and credit/LR checks or HMRC data shows continuing poor circumstances beyond the end of the agreement.

Reason and Code	Description	Evidence
6 - Outside jurisdiction debtor has been deported, or now living abroad	Debtor is outside of the UK.	Evidence to show that debtor no longer resides in the UK. Three checks over two years by Supplier plus the Authority's final check on Equifax at time of write off in case debtor re-emerges back in UK /obtains new right to remain.
7- Statute barred- debt has lapsed after 6 years due to non-communications /chasing of debt for more than 6 years.	Statute-barred.	The debt is older than six years old (from revocation or recoupment date). NB this does not apply to issue of ICOs or CCOs which are not time barred. Statute barred provisions apply only to the collection of the debt.
8 - Lost charge due to admin error by either 3 rd party or by Land Registry and assets are dissipated before the error is discovered.	Lost charge.	Copy of Land Registry document.
9-Repossession/insufficient funds for distribution	Repossession/insufficient funds for distribution.	Final Completion Statement confirming the distribution of monies or letter from the conveyancing solicitors confirming insufficient funds to redeem the mortgage and there are no surplus funds available for distribution.
10 -Property sold with negative Equity	Property sold with negative Equity.	Letter from the conveyancing solicitors confirming insufficient funds to redeem the mortgage and there are no/partial surplus funds available for distribution.
11- Unable to enforce - no supporting evidence	Unable to enforce - no supporting evidence.	Unable to locate MoJ records or evidence to support enforcement e.g. HMCTS court records confirming Sentence Order Date or conviction no longer exist due to HMCTS data retention policies.
12 - Unable to enforce - enforcement action not viable on advice of Authority, Legal or SLT/ELT or on direction of judge	Unable to enforce - enforcement action not viable.	Letter from the enforcement solicitors or the Authority or a judgment order confirming enforcement action is not viable as risks outweigh the benefits.

- 6.84 If the assessment is that the debt warrants additional recovery action (for example, a large debt or the knowledge that the Defendant has liquid Capital), the Supplier will use the sanctions available to them. In all other instances, a referral back to the Authority will be made to enable a decision to be made under one of the categories above.

Varying debt balances

- 6.85 Pre-conviction ICOs can be changed as a result of an action carried out by the Authority such as new information, changes in circumstances and Hardship Reviews. In all pre conviction cases the Authority will reassess means and notify the Supplier who will be required to calculate the new debt and provide the Defendant with a refund or requesting an Additional Payment or a revised payment amount going forward. If the Supplier receives information relating to the reassessment of an ICO, they will send this onto the Authority.
- 6.86 CCOs can be changed due to new information, changes in circumstances, Hardship Reviews and judicial apportionments. The Authority will reassess and advise the Supplier of any revised liabilities where the Defendant has approached them directly with new information and will reassess all post-conviction judicial apportionment requests or Hardship Reviews. The Authority will notify the Supplier of all revised liabilities for them to re-issue a revised CCO.
- 6.87 In post-conviction cases where the Defendant advises the Supplier directly of any changes in circumstances or new information, the Supplier will be required to verify the new information and reassess and re-issue any revised CCOs.

Scanning Capability

- 6.88 There may be occasions where photocopied documents are received by the Supplier. The Supplier must have the capability to scan the documents and input the data into their Collection System.

7. IT Systems

Debt Management Recovery System

- 7.1 The Supplier must build and maintain a Debt Management Recovery System of sufficient sophistication and flexibility to handle the scope of the requirements outlined in section 6 of this Schedule 1.
- 7.2 There is one database that will need to be migrated to the Supplier. Currently, the data required to be migrated within this database will be all those cases which are open together with closed cases up to [Redacted] of age, which is approximately [Redacted] case records.
- 7.3 The [Redacted] caseload can be broken down into case notes items, case history items, and attachments such as PDFs, which equates to around [Redacted] of data.
- 7.4 Additional collected data may need to be transferred over as an exception. A suitable exceptional individual case approach will be agreed to ensure that where necessary this data is transferred such that all information is available and an older case can be appropriately re-opened if required.
- 7.5 The Supplier is expected to build and support regular and ad-hoc reporting capabilities to provide management information (MI) / reporting data of the debt recovery functions at regular intervals.
- 7.6 The Supplier must have the ability to extract and transfer raw data to the LAA successfully.
- 7.7 The Supplier must provide sufficient payment functionality as part of this service provision, which is accessible by members of the general public, on a 24/7 basis (excluding planned outages). Their systems must also include the ability to send and receive debit and credit card payments electronically.

API Data Transfer

- 7.8 The data transfer must occur via an API from the Service Commencement Date. The purpose of this transfer is to ensure the Supplier has the relevant contribution and FDC information to carry out the debt collection duties on behalf of the Authority.
- 7.9 The sequence diagram shows the flow of transferring contributions and FDC data between the Authority and the Supplier via an API. This represents a minimum viable product required from the Service Commencement Date.

[Redacted]

7.10 Specific technical aspects of the API include:

- a. The Scheduler will run once per day between 7pm and 5am;
- b. All communication between the Authority and the Supplier must be secured with OAUTH 2.0 Mutual TLS or equivalent;
- c. Contributions and FDC data will be pushed to the Supplier consuming end points by REST API using JSON objects, with a synchronous response expected to confirm receipt;
- d. Each payload will contain data pertaining to one case ID;
- e. Each payload will initially contain a full set of case data, but this will eventually change to a delta data set; and
- f. Assuming there is a time gap between the Supplier receiving data and Supplier backend processing, an asynchronous response is expected per contribution or FDC case processed, either confirming if the record was successfully loaded into the Supplier's system or providing a detailed note why it was rejected by the Supplier's system.

7.11 The Supplier is required to work with the Authority to integrate with this approach and design and build APIs in line with the principles set out in the [government's API technical and data standards](#) documentation to receive and map the transfer of data from the Authority.

7.12 The Supplier is required to build and maintain APIs that will be highly available, reliable, testable, maintainable, and scalable, as described in the [government's API technical and data standards](#) documentation to receive and map the transfer of data from the Authority.

7.13 The Supplier is required to provide detailed API documentation as per the [government's API technical and data standards](#) before the implementation.

7.14 The Supplier is required to work in an [Agile](#) way, building and releasing iterations of the system/API that deliver incremental value.

7.15 The Supplier and the Authority must be able to notify each other when Personal Data can be purged from the respective systems in accordance with UK GDPR.

7.16 The sequence diagram represents a minimum viable product for the API for the purposes of the Contract commencement. This will not be sufficient for the implementation of the Means Test Review (MTR) policy changes or for supporting the Authority's data retention policies in line with GDPR required over the life of the Contract.

7.17 The Supplier must work with the Authority to iteratively develop the API, including the provision for a two-way data flow, to enhance user features and to meet the requirements of MTR and GDPR. All changes will be in accordance with the Change or MTR Changes process, as applicable.

Testing, Logging & Monitoring

7.18 The Supplier must provide a suitable test (production replica/mirror) environment where the integration can be tested thoroughly in a non-production setting, as described in "Provide an API test service" in the [government's API technical and data standards](#) documentation.

7.19 During the Implementation Period, the Supplier must provide a test strategy for approval by the Authority. Throughout the life of the Contract, the Supplier must maintain this test strategy and plan for any changes to the API/system that are made during the life of the Contract. This strategy and plan should be shared with the Authority for Approval and review on an annual basis.

7.20 The Supplier must provide details of their Quality Assurance testing strategies to the satisfaction of the Authority. This includes any functional, integration and performance testing strategies used in relation to testing the API initial build and any functionality enhancements throughout the life of the Contract.

7.21 The Supplier will be required to build APIs/systems with good logging, monitoring, alerting, and traceability capabilities which enable the Supplier and the Authority to react proactively to any unforeseen events.

Security

7.22 The Supplier will be required to provide an annual written assurance statement that their strategies for hosting (platform/infrastructure) and deployment of API/systems meet the standards in [MOJ Cyber and Technical Security Guidance](#).

7.23 The Supplier will be required to follow [MOJ Cyber and Technical Security Guidance](#) for APIs provided by the Supplier and all supporting systems used with the APIs.

Back-Up

7.24 A full backup of CCMT data must be taken each night.

7.24.1 Any back-up of data must be encrypted to at least [Redacted] AES standard or better.

7.24.2 The back-up media will be on a [Redacted] rotation.

7.24.3 The Supplier must ensure that media for backups are taken and stored off site in a secured location within [Redacted] of completion. In the intervening time media must be securely stored in the Supplier's fire-proof safe and protected from environmental conditions that would be hazardous to the media on which the data is being stored.

7.24.4 The Supplier must ensure the Authority is able to audit the Supplier's backup logs and records of test restores.

7.24.5 An estimated timetable for completing the restoration of the CCMT data must be provided by the Supplier within 30 minutes of the request being made.

Recovery Standards

7.25 In the event of a disaster:

- 7.25.1 Fail-over to a secondary data centre or managed service provider.
- 7.25.2 Recovery within [Redacted] of Disaster Recovery Plan being instigated.
- 7.25.3 Minimal data loss to the last back-up.

Working Practices

- 7.26 Digital services and business processes within the Authority will undergo continuous changes and improvements in accordance with Agile, iterative ways of working. The Supplier is required to work with the Authority to accommodate these changes. All required changes will be subject to the Change or MTR Changes process, as applicable.
- 7.27 During the Implementation Period, the Authority requires the Supplier to share the processes followed for software release management and incident management. The Authority must be notified of any changes to these process over the life of the Contract.
- 7.28 The Authority’s business processes are subject to policy and legislative changes. The Supplier is required to accommodate these changes in accordance with the Change process. See section 11 for potential policy changes currently being consulted on.

8. [Not used]

This section is intentionally blank.

9. The Supplier and Supplier’s Staff

- 9.1 The Supplier shall:
 - not unlawfully discriminate whether in relation to race, gender, religion, age or otherwise;
 - comply with its obligations under all relevant legislation and, in particular, the Equality Act 2010 (specifically sections 149 and 150) and the Data Protection Act 2018;
 - comply with the regulations of the Financial Conduct Authority and the Market and Competition Authority;
 - ensure that Staff comply with the National Standards for Enforcement Agents, published by the Authority in 2014 (<http://www.justice.gov.uk/downloads/courts/bailiffs-enforcement-officers/national-standards-enforcement-agents.pdf>).
- 9.2 The Supplier shall provide the Authority with a copy of its code of conduct, plus any updates as they are adopted.
- 9.3 The Supplier shall disclose details of its management structure and senior staffing levels annually, upon request from the Authority CM, or when any changes occur during the period of the Contract.
- 9.4 The Supplier shall detail and agree any sub-contracting or outsourcing arrangements they wish to enter into with the Authority CM in advance.
- 9.5 The Supplier should have a recruitment policy for filling vacancies and induction policy for new starters in order to ensure that the requirements of this Contract are met and maintained by any such new starter (as applicable). This should be shared with the Authority annually.
- 9.6 The Supplier shall ensure that the Authority has up to date details of recruitment and selection procedures, security vetting procedures and training programme for its Staff as amended from time to time. It shall also supply details of how Staff are monitored for performance, and how Staff convictions are declared.
- 9.7 The Supplier shall issue each individual authorised to execute warrants or orders with an identity card displaying a photograph of that individual and that these are carried at all times and whether demanded or not shall be shown to every person against whom the Supplier is executing the Service.
- 9.8 The Supplier’s procedures and working methods should be transparent and known to and followed by its entire Staff. Guidance should be updated regularly and communicated to all Staff.
- 9.9 The Supplier should undertake ‘on the street’ auditing of Staff and vehicles should be tracked by GPS devices. Any concerns should be raised with the Authority in writing to the Authority CM.
- 9.10 Where the Supplier engages self-employed Staff, or work is sub-contracted out, the Supplier shall not seek to transfer any responsibilities from themselves to self-employed Staff so as to dilute the Supplier’s responsibilities in respect of the Services provided to the Authority.
- 9.11 The Supplier and its Staff must comply with Sections 33 and 34 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012. These sections of the Act outline restrictions on the disclosure of information of those in receipt of legal aid. Criminal penalties applicable to individuals disclosing information in contravention to these sections are also outlined.

Supplier's Staff

- 9.12 The Supplier's Staff shall operate under the direction and control of the Supplier, who shall be responsible for their conduct and discipline at all times.
- 9.13 All Staff engaged by the Supplier shall possess the qualifications, competencies, licences and identification appropriate to the tasks for which they are employed.
- 9.14 The Supplier’s Staff should be experienced in working with the public and vulnerable groups in society.
- 9.15 The Supplier’s Staff and other employees shall at all times operate in a professional and appropriate manner. They shall be sensitive to the need to ensure they do not discriminate against anyone on the grounds of any protected characteristic outlined in the Equality Act 2010. They shall not bring the relevant procedures or the Authority into disrepute.
- 9.16 The Supplier’s Staff undertaking door step services shall be certificated, security vetted, trained in health & safety and be aware of their duties under the Human Rights Act 1998. The Supplier shall ensure the certification is renewed every two years as required by current legislation including "The Credit Services Association Code of Practice".

9.17 Staff shall have regular appraisals with their line manager to promote their development and to monitor their performance.

10. Customer Service and Complaints

- 10.1 Unless otherwise agreed in advance, outward facing IT services must be available for [Redacted] of the month (excluding planned outages) to allow Defendants to pay debts online and for the Authority to access the Supplier Collection System so they can handle Defendant calls and queries.
- 10.2 The Supplier must have telephone capacity in place to i) receive incoming calls that are/are not answered; and ii) make outgoing calls in order to handle the following:
- Defendant queries;
 - payment arrangements;
 - payments over the phone;
 - outgoing follow up calls / chaser calls;
- 10.3 A telephone number must be shown on all outgoing letters from the Supplier to Defendants. An MI oversight report – MI50 - will be required to monitor this service.
- 10.4 All customer feedback, Complaints, queries, Data Subject Access Requests (DSAR) and issues must be recorded and reported in the monthly MI report.
- 10.5 All press enquiries and external communications should be referred to the Authority CM.
- 10.6 The Supplier must have processes in place to ensure that all employees recognise Data Protection and Freedom of Information Act requests and should notify the Authority CM immediately should these circumstances arise.
- 10.7 The Supplier must adhere to an agreed Complaints' process with the Authority.

Identifying a Complaint or DSAR

- 10.8 The Supplier can treat any negative comments about any Contribution Order payments as a request to review the contribution amount for first contact but any further negative comments must be treated as a Complaint.
- 10.9 A Complaint or DSAR can be verbal, written (e-mail or letter), or made in person but, in all cases, the same consistent procedures should be followed by the Supplier.
- 10.10 When making a DSAR, a Data Subject does not need to specifically refer to the legislation. The Supplier should ensure that it and its employees have received sufficient training in order to identify when a Data Subject may make a request under Data Protection Legislation.
- 10.11 If the Supplier receives any Complaints about anything other than the Services or itself or about the Authority's policies or regulations or from a Member of Parliament, Minister or Media the Supplier shall be referred to the Authority CM in writing immediately.
- 10.12 If the Supplier receives any Complaints about itself or the Services, the Supplier shall follow the procedures outlined below.
- 10.13 If the Supplier becomes aware of any act or omission of itself that may justify a claim being made against the Supplier, or the Authority, the Supplier shall, in addition to following the Complaint procedure set out below, promptly advise the originator of the Complaint in writing to seek independent advice.

Internal Complaints Procedure

- 10.14 The Supplier shall initially handle all Complaints received through a mutually agreed internal complaints' procedure. At a minimum, the complaints procedure shall include:
- a process for informing complainants about how and to whom they should complain;
 - a process for identifying any rapidly and fairly dealing with Complaints;
 - how Complaints are recorded;
 - how to identify the cause of a Complaint and respond to it (including acknowledging Complaints, telling the complainant when they will receive a substantive response, explaining to whom they should take matters if they remain dissatisfied at any stage, providing options for redress and for correcting any underlying problem or unsatisfactory procedure or process);
 - a process for recording information to prevent any future similar Complaints;
 - identification of who has responsibility for Complaints handling (generally and ultimately, including who is responsible for Complaints made about the person who would ordinarily have ultimate responsibility);
 - the process for reviewing Complaints (what is reviewed, when and by whom and number of follow ups/tiers permitted before escalation to the Authority); and
 - the point at which is Complaint is exhausted internally and should be referred to the Authority. The Supplier should have a similar procedure to the above for the handling of DSAR.
- 10.15 The Supplier shall ensure that all of the Supplier's Staff dealing with Complaints and DSAR are adequately trained and supported in order to comply with the requirements of this Specification.
- 10.16 Within one (1) Working Day of receipt of a Complaint the Supplier shall send a letter to all complainants including the following details:
- an acknowledgement of receipt of the Complaint;
 - a description of the next steps to be taken in resolving the Complaint; and
 - contact details of the person dealing with the Complaint.

In the event of receiving a DSAR, inform the Authority in writing of the request.

- 10.17 Complaints received after 4pm on a Working Day or on a day other than a Working Day shall be deemed to have been received on the next Working Day.
- 10.18 The Supplier shall keep a central record of every Complaint received. For each Complaint, the Supplier shall record the details specified below and copies of all documentation (usually correspondence) showing how it was resolved. Documentation, notes and attachments of all Complaints received and replies sent should be held on the central record and the individual case file with a cross reference in the central record.
- 10.19 The Supplier shall review the central record at least quarterly to identify trends and to determine whether action can be taken as a result, to improve the Services being delivered. The results of these reviews must be documented and stored on the central record and should be shared with the Authority.

10.20 In relation to assurance activities, the Authority is entitled to access and take copies of this central record, and any documents relating to individual Complaints at any time. The Supplier shall provide the Authority with this information within [Redacted] Days, on request.

Complaints Escalation

- 10.21 Complaints shall be escalated and referred to the Authority in the following circumstances:
- Complaint addressed to a Member of Parliament or Minister or CEO in the Authority;
 - Complaint is about the Authority's policy or there is a threat of Judicial Review;
 - Complaint has come to the attention of the media;
 - Complaint is about the Authority's conduct;
 - Complaint has exhausted the Supplier's internal escalation process agreed with the Authority.
- 10.22 Where a Complaint is escalated in accordance with this paragraph, the Authority will use reasonable endeavours to resolve the Complaint and the Supplier shall provide all assistance required by the Authority to assist the Authority in resolving the Complaint in accordance with the Authority's Complaints Procedure.

Timescale for the Resolution of Complaints

- 10.23 The Supplier shall deal with all Complaints promptly from notification. In the letter of acknowledgement described above, the complainant must be provided with an initial estimate of the timescale for resolution of the Complaint. The complainant must be provided with a regular update on the status of the Complaint (including any changes to the likely timescale for resolution) and in any event, not more than 5 Working Days from the previous update. Substantive complaint responses should be provided within [Redacted] of receipt.

Timescale for the Resolution of Complaints & Correspondence received by the Authority

- 10.24 The Supplier shall provide the Authority with any reports or copies of correspondence within 24 hours to enable the Authority to deal with any Complaints sent directly to the Authority by the complainant.

Reporting Complaints

- 10.25 The Supplier shall record details of every Complaint received. This will form a Complaints Log showing the following information:
- complainant's name;
 - Complaint reference number;
 - MAAT reference no;
 - owner of the Complaint;
 - delivery type e.g. letter, e-mail etc;
 - date Complaint received;
 - description of the Complaint;
 - date holding letter was sent;
 - date full response was sent;
 - equalities monitoring data – complainant's age, gender and ethnicity;
 - action taken; and
 - whether the Complaint was justified or unjustified.
- 10.26 In addition to maintaining the Complaints Log the Supplier shall collate Complaints and carry out an analysis of their root cause at least once a quarter.
- 10.27 This analysis shall include:
- rolling volume of Complaints broken down by quarter;
 - rolling volume of Complaints upheld, partially upheld and not upheld by quarter;
 - a rolling summary of Complaints by reason category broken down by quarter;
 - an investigation into the cause/ findings of any Complaints with details reported monthly;
 - recommendations to improve the level of service offered to Defendants; and
 - a plan setting out all actions necessary to address the causes of justified Complaints within a period of three months.

11. Legal Aid Means Test Review

- 11.1 Current estimates suggest that Crown Court Means Testing policy changes resulting from the Legal Aid Means Test Review consultation will be implemented by the Authority, during the life of this Contract and the Supplier is expected to plan for consequential changes that will take place during the Contract Term. The MoJ published its response to the Means Test Review consultation in May 2023, outlining the policies that it will proceed to implement. Further detail can be found at the following link:
<https://www.gov.uk/government/consultations/legal-aid-means-test-review>
- 11.2 The Authority reserves the right to change the requirements under this Contract, especially in respect of the thresholds and provisions for calculating the contributions as well as the forecasted volumes of work and administrative costs, to reflect the outcomes of the Legal Aid Means Test Review (MTR). The Supplier will be required to implement changes to its digital systems and processes in accordance with the outcomes of the Legal Aid Means Test Review (each such Change being an MTR Change). The procedure whereby the Authority requests an MTR Change is set out in clause F7 of the Contract.
- 11.3 Table A1.6 below provides a comparison between the current scheme and the impact of key policy proposals from the MTR, as a non-exhaustive guide to the likely scope of MTR Changes, which the Supplier will be required to successfully implement.

Table A1.6 MTR key policy proposals

Type of Case	Current scheme	Policy changes to be implemented following the MTR
--------------	----------------	--

<p>Pre conviction –</p> <p>Criminal proceedings in the Crown Court – committed, sent, or transferred for trial</p>	<p>Income Contribution Order (ICO)</p> <p>An ICO is issued by the Authority and is based on the Defendant's household disposable income.</p> <p>Defendants liable for an income-based contribution will either pay for the life of the case or for six months, whichever is the shortest. The contribution is 90% of household disposable income and the minimum monthly contribution is [Redacted]. This may also be limited to the maximum income contribution that is set, depending on the type of case.</p> <p>Where Defendants fail to provide sufficient evidence to support the details provided in their legal aid application, an uplift in the sums due via an Income Evidence Sanction (IES) will be applied by the Authority until the evidence is received.</p> <p>All Defendants who are acquitted will be refunded any monies paid with [Redacted] compound interest.</p>	<p>Defendants liable for an income-based contribution will either pay for the life of the case or eighteen months, whichever is the shortest. The contribution will be on a sliding scale of three bands of [Redacted] of household disposable income and the minimum monthly contribution is [Redacted].</p> <p>All Defendants who are acquitted will be refunded any monies paid with rate of interest linked to base rate which will be reviewed every [Redacted] in line with reviewing the means test as a whole.</p>
<p>Post conviction –</p> <p>Sentenced by Crown Court and found guilty or partially guilty</p>	<p>Capital Contribution Order (CCO)</p> <p>Issued to Defendants with disposable Capital & Equity above [Redacted] who fail the Authority means test and are subject to an ICO or are not passported e.g. not on benefits.</p> <p>A CCO is calculated on the basis of based on the FDC (see below), balancing any monies paid to date and whether any outstanding costs remain. This is issued by the Supplier after completion of a K&E Check confirming available Capital and Equity assets in the Defendant's household and is undertaken either by the Authority, the Supplier or both. When there is still a financial liability outstanding after conviction, then recovery of the balance will be made from Capital/Equity.</p> <p>Recoveries of post-conviction debt can still be pursued against the pre conviction ICO if these are still outstanding at the point of conviction and there are Capital and Equity assets above [Redacted].</p> <p>[Redacted] Compound interest on outstanding post-conviction debt may be applied.</p>	<p>Issued to either:</p> <ul style="list-style-type: none"> non-passported convicted Defendants with disposable Capital & Equity above [Redacted], who may also have failed the means test and are subject to an ICO or passed the means test and were not previously subject to an ICO; or convicted Defendants who, although passported, have a chargeable property. <p>Interest will be charged at a rate of interest linked to base rate which will be reviewed every [Redacted] years in line with reviewing the means test as a whole.</p>

Appendix A – Process Flow Diagrams

[Redacted]

Appendix B – Capital & Equity Initial Sift Business Rules

Rule 1: Identify convicted income contribution cases & non passported post conviction cases (convicted outcomes) (exclude appeals - Capital not relevant)

Income contribution paid (A)	Income contribution cap (B)	If A is larger than B no check required
[Redacted]	[Redacted]	No checks
[Redacted]	[Redacted]	Continue to look at Capital position
[Redacted]	[Redacted]	Continue to look at Capital position

Rule 2: Review case type to exclude

Appeals	Capital is not relevant to these types of cases
Committals for Sentence	Would only be included as anomalous data, but do not need

Rule 3: Have assets of [redacted] or less been declared? (This filters out those with no assets at all, and those with restrained assets of [redacted])

Any assets declared over [redacted], a K&E Check is potentially required

Rule 4: Has enough Capital+ Equity already been declared?

A- Equity declared	B- Capital items declared	Total assessed Capital assets	Less 30K threshold	Income contribution cap		
Equity amount	Individual items in feed Total Capital amount	Add A & B	deduct 30 k	Figure from feed	If sufficient declared to cover remainder of 90th percentile figure	No K&E Check required
					If insufficient declared to cover remainder of 90th percentile figure	Proceed to K&E Check

Categories

Category 1	Enough already - either through income contributions paid and /or Capital & Equity declared	Stop Here
Category 2	K&E Checks already been undertaken by the Authority - will see verified figures in data feed	Stop Here
Category 3	Insufficient collected / declared to cover 90th percentile cap (but [Redacted]) = K&E Checks required	Pursue checks
Category 4	Once Final Defence Costs (FDC) received - if higher than 90th percentile cap then revisit whether sufficient declared / identified	Revisit post FDC

Outputs following Category 3 cases checks

Declared cap/Equity below [Redacted] & evidenced		No suggestion of further Capital & Equity found	CCO = nil		
Declared cap/Equity above [Redacted] but not evidenced	Monies paid to date are less than income contribution cap	No suggestion of further Capital & Equity found	Evidence missing and material to contribution	Chase Capital evidence	Refer to Authority if not rec'd - Capital sanction may be appropriate
Declared cap/Equity above [Redacted] plus income contribution paid but not evidenced	Monies paid to date are less than income contribution cap	No suggestion of further Capital & Equity found	Evidence missing and material to contribution	Chase Capital evidence	Refer to Authority if not rec'd - Capital sanction may be appropriate
Any declaration where costs not covered		Undeclared assets identified	Referral to Authority	Further action may be required (from Defendant /Supplier / Courts/Authority)	Authority to confirm final figure for available* Capital & Equity

		Undeclared partner identified	Referral to Authority	Further action may be required (from Defendant /Supplier / Courts/Authority)	Authority to confirm final figure for available* Capital & Equity
		Undeclared property identified	Referral to Authority	Further action may be required (from Defendant /Supplier / Courts/Authority)	Authority to confirm final figure for available* Capital & Equity

* Available Capital= assessment of whether anything else is material e.g. 1 bank account and no property= no further action necessary

Appendix C – Business Rules for Re-Assessment of Pre Conviction Contributions

[Redacted]

Intentionally blank.

Debt Collection and Enforcement Services contract signature

Final Audit Report

[Redacted]

Created:	[Redacted]
By:	[Redacted]
Status:	[Redacted]
Transaction ID:	[Redacted]

"Debt Collection and Enforcement Services contract signature" History

Document created by [Redacted]

Document emailed to [Redacted]

Email viewed by [Redacted]

Signer [Redacted]

 Document e-signed by [Redacted]

- Agreement completed.
[Redacted]

Debt Collection and Enforcement Services contract signature

Final Audit Report

[Redacted]

Created:	[Redacted]
By:	[Redacted]
Status:	[Redacted]
Transaction ID:	[Redacted]

"Debt Collection and Enforcement Services contract signature" History

Document created by [Redacted]

Document emailed to [Redacted]

- Email viewed by [Redacted]

 Signer [Redacted]

Document [Redacted]

- Agreement completed.
[Redacted]