MASTER SERVICE AGREEMENT

This Master Service Agreement (the "Agreement") dated Saturday, 11 April 2020 ("Effective Date") is known by its reference **ACFUK-MSA-Test Centre Management**

This Agreement consists of the included general Terms and Conditions, with Supplemental Conditions (if any), and all Schedules appended to them or which are subsequently signed by the Parties and which refer to this Master Services Agreement (including any Fee's referred to in Schedules), the Service Level Agreement and the Orders that refer to this Master Services Agreement (collectively, the "Master Services Agreement").

BETWEEN

The Secretary of State for Health and Social Care

acting as part of the Crown through the Department of Health and Social Care

whose registered office is at 39 Victoria Street, Westminster, London, SW1H 0EU.

(the "Client")

– AND –

ACF Technologies (UK) Limited

a company registered in in England (no 06460227) whose registered office is at Technology House, 48-54 Goldsworth Road, Woking, Surrey, GU21 6LE, United Kingdom. ACF Technologies (UK) Limited is a wholly owned subsidiary of ACF Technologies Inc, registered in Asheville, North Carolina, and together are referred to as "ACF".

(the "Vendor")

WHEREAS

The Vendor is the owner of the Software (as hereinafter defined);

The Vendor wishes to grant a Licence (as hereinafter defined) to the Client ("Licensee") to use the Software, provide Support (as hereinafter defined) in connection with such Licence grant, and Licensee wishes to accept such a grant of Licence and obtain support, on all terms and conditions set forth in this Agreement.

The Vendor wishes to provide ancillary services in connection with the Licence grant;

The Client is of the opinion that the Vendor has the necessary qualifications, experience and abilities to provide services to the Client;

NOW THEREFORE

In consideration of the mutual promises and covenants herein, the sufficiency of which is hereby acknowledged, the parties agree to the Terms and Conditions within.

IN WITNESS WHEREOF, the parties have executed this Agreement by their duly authorized representatives as of the date first set forth above.

for and on behalf of The Secretary of State	for and on behalf of **ACF Technologies (UK) Limited**
[redacted]	[redacted]
(Authorised Signature)	(Authorised Signature)
[redacted]	[redacted]
(Printed Name)	(Printed Name)
Procurement Category Manager (ICT & Digital) for DHSC	VP BUSINESS DEVELOPMENT
(Title)	(Title)
11 APRIL 2020	11TH APRIL 2020
(Date)	(Date)

CONTENTS

1. Definitions

1.1. "**Business Day**" means Mondays through Fridays, inclusive, but does not include national, public, or bank holidays in the country or locality where the relevant action is to be taken.

1.2. "**Charges**" means the fees payable for Software or Services under this Master Services Agreement and as further defined in the Service Schedule(s), the Supplemental Conditions and/or the Order Form(s).

1.3. "**Confidential Information**" shall mean all confidential and proprietary information, whether of a technical, business or other nature, including without limitation, inventions, know-how, trade secrets, methods and information, business plans, finances and other business affairs, disclosed by the Vendor to the Licensee in tangible form.

1.4. "**Client**" refers to the entity who's details are provided within this Agreement, and who shall be subject to its terms.

1.5. "**Dispute**" means any disagreement, conflict or claims arising out of or in connection with the Agreement or its validity.

1.6. "**Documentation**" shall mean any product descriptions, user manuals, training materials and other documents related to the Software (inclusive of any updates and/or upgrades) provided by ACF to the Licensee.

1.7. "**Hardware**" means the hardware components identified in EXHIBIT A hereto.

1.8. **"Hosting Services"** means the hosted environment in EXHIBIT A hereto.

1.9. "**Licence**" shall mean the instrument governing the use of the Software, as per the End User Licence Agreement ("EULA") contained within this Agreement.

1.10. "**Master Services Agreement**" has the meaning given to it on the first page and is also known as the "Agreement".

1.11. "**Object Code**" shall mean the computer software code which results from the translation or processing of source code by a computer into machine executable or intermediate code, which code is not readily understandable to a human being but is appropriate for execution or interpretation by a computer.

1.12. "**Order**" means an official document provided by the Client that instructs the Vendor to supply Software and/or Services under the terms of this Agreement, according to the Fee structure set out by the Vendor's Quote.

1.13. "**Party**" means either ACF or the Client; "**Parties**" means both ACF and the Client.

1.14. "**Quote**" shall mean the Vendor's formal instrument to indicate the cost of the Software and/or Services.

1.15. "**Schedule**" shall mean the enclosed addendums to this Agreement to which describes the Software and Services being provided.

1.16. "**Service**" means each service as described in the relevant Schedule and, as the case may be, further specified in any applicable proposal document from ACF, or Order from the Client.

1.17. "**Service Level Agreement**" means the level to which the Service shall be performed, and is described in the supporting Schedule within the Agreement defining the service levels applicable to that Service.

1.18. "**Software**" shall mean ACF's software as more fully described within the supporting Schedules hereto, including any supporting Documentation.

1.19. **"Software as a Service (SaaS)"** shall mean a software licensing and delivery model in which software is licensed on a subscription basis.

1.20. "**Support**" shall mean those services provided by ACF to Licensee with respect to the Software and/or Hardware, if applicable, and as specified within the supporting Schedules hereto.

1.21. "**User**" means any individual who is permitted to access the Software, consuming a Licence. Service purchased by the Customer

1.22. "**Vendor**" refers to ACF, the supplier of the Software and Services.

2. Term and Termination

This Agreement will commence on the Effective Date and will continue for six (6) months. This Agreement will be automatically renewed for successive three (3) month term, unless either party gives notice to the other party not less than thirty (30) days prior to expiration of the initial term or any renewal term that it does not intend to renew this Agreement, or unless this Agreement is otherwise terminated in accordance with this Section.

Either party may terminate this Agreement if the other party is in material breach or default of any obligation hereunder, and such breach or default is not cured (or, if cure is not practical within thirty (30) days, commenced cure) within thirty (30) days of written notice from the other party.

Effective immediately upon termination of this Agreement, ACF will cease to provide any Support to Licensee.

In the event of termination or expiration of this Agreement for any reason, the following Sections shall survive termination: Fees, Payment, Limited Warranty; Indemnification; Limitation on Liability. Consequential Damages Waiver, Trademarks and Proprietary Rights, Confidentiality, Notices.

3. Grant of Licence; Acceptance

3.1. ACF hereby grants to Licensee a non-exclusive, non-transferable, non-sublicenceable Licence to use and install the Software, in machine-readable Object Code form, and to use the Software provided by ACF for Licensee's business purposes.

3.2. Licensee shall not modify, change, create any derivative works, decompile, disassemble or otherwise reverse engineer the Software, or make any copies of the Software.

3.3. ACF hereby grants to Licensee a Licence to use the Hardware in connection with Licensee's use of the Software.

3.4. Upon completion of installation of the Hardware and Software by ACF, Licensee, shall test the Hardware and Software to determine whether they perform substantially in accordance with the Documentation. Licensee will notify ACF, in writing that it is accepting or rejecting the Hardware and Software within fifteen (15) days after installation is completed. Any notice of rejection shall set forth the grounds for rejection. ACF shall use its best efforts to remedy any failures of the Hardware and Software to perform substantially in accordance with the Documentation within ten days from the date of the

rejection notice. When the Hardware and Software have been accepted, Licensee shall issue a written confirmation of acceptance to ACF ("Acceptance").

3.5. In the case of a "SaaS" Agreement model the Licensee only retains the right to use the Software for the term.

4. Fees

In consideration of the Licences granted hereunder, and the other covenants of ACF hereunder, Licensee agrees to pay ACF the fees set forth in EXIBIT A. All fees as set forth in EXIBIT A are exclusive of any and all taxes and other expenses, such as shipping, freight, and insurance expenses.

5. Payment

Licensee shall remit payment when requested within thirty (30) days from the date of ACF's invoice. Invoices will be raised against agreed payment gateways as set forth in EXIBIT A, as per the "Payment Schedule".

6. Support and Maintenance

On payment of the associated fees ACF shall make available to Licensee Support and Maintenance for the Software and/or Hardware, where applicable, as set forth in EXIBIT B.

7. Training

ACF shall provide a training session for the IT team of the Licensee and to managers that will be using the software. Training will include supporting information for IT to install in the future other locations independently (if requested) and training for managers to train the staff on all needed operational aspects of the software. ACF and Licensee may arrange additional training by mutual agreement.

Training will be held on consecutive days, not exceeding the number of days stated in Exhibit A. ACF has the right to charge for an additional whole day(s) plus travel and subsistence costs. If subsequent Training Days are required, these will be charged at the same rate as proposed herewith plus travel and subsistence.

8. Installation

8.1. Installation will be held on consecutive days, not exceeding number of days within this proposal. ACF has the right to charge for an additional whole day(s) plus travel and subsistence costs.

8.2. Supply/Provisioning of server to host the Q-Flow® software will be the responsibility of the Customer, unless otherwise stated within the scope and subject to quote.

8.3. Supply/Provisioning of the media PC(s) to play the digital content will be the responsibility of the Customer – and it is the responsibility of the Customers to ensure the media pc is compatible with the LCDs, unless otherwise stated within the scope and subject to quote.

8.4. Provisioning of the central PC to host Q-Flow server licences will be the responsibility of the Customer, unless otherwise stated within the scope and subject to quote.

8.5. Supply/Provisioning of Microsoft SQL Server to be used on the central PC will the responsibility of the Customer, unless otherwise stated within the scope and subject to quote.

8.6. All structured cabling, power points, channelling of surfaces such as floors, walls, etc., including termination and testing of cables, should be provided by customer's electrical contractor. Our installers will be responsible for mounting and commissioning equipment, as offered in this proposal.

8.7. Installation costs are based on business working hours (9:00AM – 5:00PM) during weekdays only.

8.8. Fitment of any ceiling bracket for LCD use will be to a maximum height of 2.6 metres.

8.9. Cost of installation is based on "site unseen" unless a site survey has been paid for.

9. Appointment of Representatives

Each party shall designate an employee to represent that party for purposes of any communications between the parties regarding this Agreement.

10. Limited Warranty; Indemnification; Limitation On Liability

10.1. Limited Warranty. ACF warrants and represents to Licensee that for a period of 1 year after Acceptance of the Software to Licensee ("Warranty Period"), the Software shall perform substantially in accordance with the Documentation, when used in accordance with the Documentation. ACF's sole obligation to Licensee during the Warranty Period shall be to repair or replace defective Software, at ACF's option, provided the defects are those for which ACF is responsible. ACF will have no responsibility or liability whatsoever for claims of defect or damages arising from (i) the use of the Software not in compliance with its specifications or the functional description provided in the Documentation; (ii) the unauthorized combination of the Software with third party components or software; or (iii) unauthorized or improper alteration or repair of the Software.

10.2. ACF does not provide any warranty with respect to the Hardware. The Hardware is subject to its own warranty, as set forth in its specifications. However, ACF warrants and represents to Licensee that the Software and Hardware installation services provided by ACF will be provided in accordance with the highest degree of professional skill and competence

10.3. Proprietary Rights Indemnity. Subject to the limitations set forth herein below, ACF shall indemnify, defend and hold harmless Licensee with respect to any claim, suit or proceeding (each, a "Claim") brought against ACF to the extent it is based upon a claim that the Software Licenced pursuant to this Agreement infringes upon any U.S. patent, trademark, copyright or trade secret of any third party; provided, however, that Licensee (i) promptly notifies ACF in writing of such Claim; and (ii) gives ACF the right to control and direct the investigation, preparation, defence and settlement of such Claim. If the Software is, or in ACF's opinion, might be held to infringe as set forth above, ACF may, at its option, (i) procure for Licensee the right to continue to use the Software under this Agreement; (ii) replace or modify the Software (or any portion thereof) under this Agreement so that it will be non-infringing; or (iii) if neither (i) nor (ii) are possible, ACF shall have the right to terminate this Agreement and refund to Licensee the pro-rata Licence fees. The foregoing indemnity shall not apply to any Claim(s) based upon or arising from (i) the use of the Software not in compliance with its specifications or the functional description provided in the Documentation; (ii) the combination of the Software with third party components or Software, where the Software standing alone, would not have infringed upon third party rights; or (iii) unauthorized or improper alteration or repair of the Software. THE RIGHTS GRANTED TO LICENSEE UNDER

THIS AGREEMENT SHALL BE LICENSEE'S SOLE AND EXCLUSIVE REMEDY FOR ANY ALLEGED INFRINGEMENT OF ANY PROPRIETARY RIGHT.

10.4. THE REPRESENTATIONS AND WARRANTIES SET FORTH CONSTITUTE THE ONLY REPRESENTATIONS AND WARRANTIES UNDER THIS AGREEMENT WITH RESPECT TO THE SOFTWARE. ACF MAKES AND LICENSEE RECEIVES NO OTHER REPRESENTATIONS AND WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, AND ANY IMPLIED WARRANTY OR CONDITION OF FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, MERCHANTABLE QUALITY OR NON-INFRINGEMENT. BOTH PARTIES ACKNOWLEDGE THAT THE MUTUAL PROMISES CONTAINED HEREWITHIN REFLECT THE ALLOCATION OF RISK SET FORTH IN THIS AGREEMENT, THAT BOTH PARTIES WOULD NOT ENTER INTO THIS AGREEMENT WITHOUT THESE LIMITATIONS ON LIABILITY, AND SUCH LIMITATIONS SHALL BE GIVEN FULL EFFECT EVEN IN THE EVENT THAT ANY OF THE REMEDIES PROVIDED IN THIS AGREEMENT ARE DEEMED BY A COURT OF COMPETENT JURISDICTION TO HAVE FAILED OF THEIR ESSENTIAL PURPOSE.

10.5. Limitation of Claims. No claim, regardless of form, which in any way arises out of this Agreement, may be brought more than twelve (12) months (1 year) after the basis for the claim becomes known to the party desiring to assert it.

10.6. ACF further represents and warrants that it has not paid a fee nor given any compensation to an employee of Licensee or any third party in order to secure the award of this Agreement.

11. Consequential Damages Waiver

Without limiting the above, neither Licensee nor ACF, nor any of their respective affiliates and representatives shall have any liability with respect to its obligations under this Agreement for any loss of profits or other economic loss or for indirect, consequential, special, exemplary, or incidental damages of any kind, regardless of the form of action, whether in contract, tort (including negligence), strict product liability or otherwise, even if such party has been advised of the possibility of such damages. In no event will ACF or its affiliates or representatives be liable for costs of procurement of substitute products by Licensee.

12. Trademarks and Proprietary Rights

12.1. During the term of this Agreement, ACF hereby grants to the Licensee, subject to the terms and conditions of this Agreement, a limited, royalty-free, non-exclusive, non-transferable, non- sub-licensable, right and Licence to use and display, solely in connection with Licensee's use of the Software, ACF's trade names, trademarks, service marks and associated logos (the "Marks"). No

other use of ACF's Marks shall be made by Licensee except as expressly granted hereunder, without the prior written consent of ACF.

12.2. ACF will retain all right, title and interest in and to its Marks, and all goodwill associated with use of such Marks will inure solely to the benefit of ACF. All use of ACF's Marks by Licensee shall conform to good trademark usage practice or any reasonable trademark usage guidelines or instructions that ACF may provide Licensee from time to time. No Licences are hereby granted by ACF to the Licensee with respect to the Licensor's Marks except for those expressly set forth in this Agreement.

12.3. Licensee acknowledges that the structure and organization and code of the Software are proprietary to ACF and that ACF retains exclusive ownership of the Software, the Documentation and the Marks. Licensee will take all reasonable measures to protect ACF's proprietary rights in the Software. Except as provided herein, Licensee is not granted any rights to patents, copyrights, trade secrets, trade names, trademarks (whether registered or unregistered), or any other rights or Licences with respect to the Software.

13. Confidentiality

Mutual confidentiality is assured and agreed by way of ANNEX D: MUTUAL NON-DISCLOSURE AGREEMENT.

14. Assignment.

Licensee may not assign, in whole or in part, this Agreement, the Software or any right or obligation under this Agreement to anyone, without ACF's prior written consent, which consent will not be unreasonably withheld. ACF may assign this Agreement or any rights or obligations herein without the consent of Licensee.

15. Complete Agreement.

Each party acknowledges that it has read and understands this Agreement and agrees to be bound by its terms. The parties further agree that this Agreement, including the Exhibits hereto, represents the complete understanding between the parties relating to the Software, Hardware and Services, which supersedes and merges all prior proposals, understandings and all other agreements, oral or written, between the parties. This Agreement may not be modified or altered except by written instrument duly executed by both parties.

16. Notices.

All notices, authorisations, and requests in connection with this Agreement shall be deemed given: (i) within five (5) days of the day on which they are deposited in the UK mail, postage prepaid, certified or registered, return receipt requested; (ii) within one (1) day of being sent, if by overnight mail or air express courier, charges prepaid; or (iii) on the day of transmittal if sent by facsimile, email, modem or other means of mutually accepted electronic communication, with confirmation of receipt; and addressed to the parties as set forth above.

17. Governing Law & Jurisdiction.

This Agreement and performance hereunder shall be governed exclusively by the laws of England and Wales.

18. Force Majeure.

Neither party shall be liable for any act, omission, or failure to fulfil its obligations under this Agreement if such act, omission or failure arises from any cause reasonably beyond its control, without its fault or negligence, and which could not reasonably have been remedied, such as, but not limited to, acts of God, reasons of fire and floods. The party unable to fulfil its obligations shall immediately notify in writing the other party of the reasons for its failure to fulfil its obligations and the effect of such failure and shall use its best efforts to reduce and overcome within a reasonable time, the effects of the Force Majeure event which affect the performance of its obligations.

19. Waiver.

The waiver or failure of either party to exercise any right provided for herein shall not be deemed a waiver of any further right hereunder.

20. Severability.

If any provision of this Agreement is invalid, illegal or unenforceable under any applicable statute or rule of law, it is to that extent to be deemed omitted, and the remaining provisions shall not be affected in any way.

21. Headings.

The headings contained in this Agreement and the Exhibits attached hereto are intended for convenience or reference only and shall not control or affect the meaning or construction of any provisions of this Agreement.

22. Independent Contractors.

The parties hereto are and shall remain independent contractors. Nothing herein shall be deemed to establish a partnership, employment, joint venture, or agency relationship between the parties. Neither party shall have the right to obligate or bind the other party in any manner to any third party.

23. Counterparts.

This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

24. Exhibits.

All Exhibits which are annexed to this Agreement are expressly made a part of this Agreement and are incorporated herein by this reference. All references to this Agreement shall be deemed to refer to and include this Agreement and all such Exhibits, as may be amended from time to time in writing. In the event of an inconsistency between the body of this Agreement and an exhibit, the terms in this Agreement shall prevail.

END OF AGREEMENT (SEE FOLLOWING EXHIBITS)

EXHIBIT A: FEES

All prices are in Sterling, and exclude VAT.

The below are fees are in relation to providing the Client with the following requirement:

ACF will provide an appointment management software solution and associated services, including, and not limited to:

- Software Licenses to
  - Access for Deloitte UI to consume our API to search for a test centre and book an available appointment online
  - Access for Deloitte UI to consume our API to locate a test centre local in distance to the postcode provided
  - Access to Q-Flow UI to allow test centre supervisors to manage the appointment availability at test centres
  - Provide access to Deloitte for access to data for reporting purposes
- Hosting Environments to
  - Support the above software solution, according to current known demands, estimated at 100-150 transactions per second, potentially up to 10 million appointments per month in high demand periods.
- Professional Services in order to:
  - Deliver to the above requirement
  - Support the above requirement

A formal Quote will be provided by ACF to describe the solution, and calculate total values based on quantities required of each item. This Agreement will supersede any dispute where the quotation does not match the values contained within EXHIBIT A.

1. Software Licences

Software licenses will be issued free of charge for the first six (6) months of production usage from Go Live. Additional usage, after the initial six (6) month period, will be charged on a 3-month basis and detailed below.

Licence	Unit	Cost
Q-Flow Test Centre License*	[redacted]	[redacted]
		[redacted]

* required Q-Flow server modules are marked below as Service Required:

Queue & Route	Not Required	Exchange Bridge	Not Required
Calendar	Service Required	Core API	Service Required
Advanced Calendar	Service Required	Brochure POD API	Not Required
Herald	Not Required	UXC	Not Required
Intercom	Not Required	Advanced UXC	Not Required
Brochure POD	Not Required	Planner	Not Required
BPM	Not Required	Planner API	Not Required
Advanced QM	Not Required	Kiosk Analytics	Not Required
Connect	Service Required	Kiosk Analysis License	Not Required
Online Forms	Not Required	Insight	Not Required

2. Professional Services

2.1. ACF will provide professional services free of charge up to a maximum of [redacted]. Additional professional services will be provided at a flat rate fee of [redacted], during normal business hours (09:00 to 17:00, Monday to Friday). Where appropriate an hourly rate of [redacted] will be charged.

2.2. Professional services provided outside of normal business hours will be charged as a variation order at:

2.2.1. [redacted] normal rate for outside of normal business hours and Saturdays.

2.2.2. [redacted] normal rate for Sundays & Public Holidays.

3. Hosting

ACF provide a managed service where Q-Flow is hosted on the secure Microsoft Azure cloud platform. The provision includes Virtual Machines and appropriate network services, that are sized for your individual requirements.

Hosting provision [redacted] per month according to the current expect demand. Demand is currently estimated at 100-150 transactions per second, potentially 10 million appointments in high demand periods.

4. Support and Maintenance

Support and Maintenance services are provided by ACF under the terms provided in Exhibit B of this Master Service Agreement. These costs are included on the solution licensing costs and covers 8am to 8pm cover.

24x7 support is available – the costs for which are as follows and based upon a 3-month period:

Licence	Unit	Cost
24 x 7 Q-Flow Support	[redacted]	[redacted]
		[redacted]

5. Incurred Costs

ACF reserve the right to pass on any costs incurred in the course of implementing the Software or Services within this Master Service Agreement, plus a [redacted] administration fee.

This includes, but is not limited to, economy class travel, vehicle hire, mileage expenses, accommodation, sustenance or equipment procured to render the implementation successful. These charges will be provided on a monthly basis.

Additional costs include, but not limited to:

Service	Cost
SMS reminders & notifications (cost per SMS)	[redacted]
Bing Location Lookup – initial block of 6 million transactions	[redacted]
Bing Location Lookup - per additional 1,000 transactions	[redacted]

6. Payment Schedule

Milestone	Value
On Purchase Order	[redacted]

On receipt of the official Client Purchase Order	[redacted] Azure hosting
On Production Software Licences Activation Where ACF provide an Activation Key, in response to an Activation Key Request, which is generated on installation of the XML Licence file *All charges are upfront*	24x7 Support Costs [redacted]
(Optional) SMS consumption charges *Charged monthly in arrears*	[redacted] per SMS
BING API GEO lookup *Charged monthly in arrears*	[redacted] per [redacted] transactions
Hosting *All charges are upfront*	[redacted] per month
Quarterly from the six (6) month free period *All charges are upfront*	Test Centre Licenses [redacted] 24x7 Support Costs [redacted]
Monthly *All charges are in arrears*	[redacted] of Professional Services consumed.

END OF EXHIBIT A

ACF have provided an indicative cost breakdown at the end of section

EXHIBIT B: SUPPORT AND MAINTANENCE AGREEMENT

1. Definitions

1.1. "**Error**" means any defect, including but not limited to a security defect, performance problem or other defect in the Software and/or Hardware which prevents the Software and/or Hardware from performing in accordance with the Documentation.

1.2. "**Incident**" shall mean an instance of an Error reported to ACF by Licensee based on a material failure of the Software to confirm with the product specifications.

1.3. "**Incident Category**" shall mean the assigned priority to the Incident or Service Request

1.4. "**Maintenance**" means the provision by ACF to Licensee of New Releases and Upgrades of the Software.

1.5. "**New Release**" means a major product version release of the Software Licenced under this Agreement.

1.6. "**Patch**" means a fix to specific Software deficiencies that occur within the Licensee's specific environment. A Patch shall be made available only for the current release.

1.7. "**Upgrade**" means a minor product version release of the Software Licenced under this Agreement.

1.8. All other capitalized terms used herein shall have the same meanings as set forth in the Agreement.

2. Clauses

2.1. Maintenance and Support plans may be ordered by Licensee only pursuant to the terms and prices as set forth in Exhibit A, but specifically, ACF, or any contractor ACF shall so appoint ("Contractor"), shall provide Support and Maintenance for the Software and/or Hardware, if applicable, at no additional charge, for a period starting on the date of Acceptance and ending one (1) year thereafter (the "Initial Support Period"). Following the Initial Support Period, Licensee may, at its option, renew Support for additional periods of one (1) year each. The annual Support fees are set forth in the attached Exhibit A.

2.2. ACF or Contractor shall, upon receipt of a Service Request from Licensee, proceed as follows:

2.2.1. Validate the Service Request and priority (Incident Category) from Licensee.

2.2.2. Validate information regarding the alleged Error provided by Licensee. Each Error reported will be assigned a Service Request number (case identifier).

2.2.3. Provide a Patch or otherwise remedy the alleged Error within the time frame set forth.

2.3. Time Frame. See SLA below.

2.4. Notwithstanding the above, ACF or Contractor shall provide Support only for the latest version of the Software and the version immediately prior to the latest version.

2.5. Support Coverage. ACF or Contractor shall provide telephone and e-mail support lines for Licensee to call for questions and technical issues regarding the Software (which shall only include the latest version of the Software and the version immediately prior to said latest version) and/or the Hardware as defined in the Service Coverage section below.

2.6. ACF shall provide to Licensee, at no additional charge, any Upgrades and New Releases of the Software required to maintain support as set forth in article 1.5, including associated Documentation. If ACF does, in fact, release any New Releases or Upgrades to the Software, Licensee shall either replace the then-existing Software with the Newly Released or Upgraded Software within six (6) months from the release of each, or shall, within three (3) months from the release, send ACF a written request (Purchase Order) for the performance of such replacement by ACF based on installation fees as set forth in Exhibit A. All New Releases and Upgrades shall be subject to the same licensing terms as are applicable in this Agreement. In the event that Licensee fails to install the Upgrade or New Release, ACF may withhold any Support services from Licensee.

3. Support Contact Information

3.1. Telephone number for support: [redacted]

3.2. Email address for support: [redacted]

4. Incident Management

An incident may be raised by way of email or telephone call, as per the provided Support Contact Information.

The incident will be logged by ACF's UK based Support Desk, and communication with the Licensee shall be as follows:

4.1. Customer will receive a standard notification email informing them of the incident number.

4.2. Following categorization of the incident a further email shall be issued confirming the priority and the agent to which the incident has been assigned.

4.3. Ongoing communication will be 'as required' using the Client's supplied contact details.

5. Problem Management

In the event an incident has occurred multiple times, affects multiple clients or affects multiple systems, ACF will escalate internally to Second, or Third line support facilities. This will allow further expert investigation, diagnosis and resolution of the affecting incident/s. The aim of the escalation being to identify the root cause and implement either reactive or proactive fixes to ensure ongoing running of the system.

6. Change Management

Should an incident or problem result in a requirement for change, this will follow ACF standard change process. Requirements and scope definition will be agreed with client before being presented to the internal ACF change approval board for implementation. Upon agreed timescales and implementation decisions the client shall be informed of any planned maintenance to implement the change and/or other associated impacts such as cost or resource requirements from the client.

7. Planned Maintenance

The client will be informed of any planned maintenance to software or hardware where applicable. The timescales for implementation will be agreed with the client and notification issued at least 24 hours prior to commencement.

Emergency maintenance can be conducted with at least 2 hours' notice to client, this will only occur in the instance event monitoring has alerted the service desk to a severity 1 incident that will occur should proactive measures not be taken to resolve.

8. Major Incident Handling

The following criteria will be used to determine whether an incident will be managed using the Major Incident Handling procedure:

8.1. Any incident recorded as having a high severity level and high impact level where ACF and the Client deem the service not fit for purpose.

8.2. Any incident recorded as having a high urgency level, with a projected recovery time that may result in a failure to meet one or more service level objectives.

8.3. Any incident where the senior IT management team and the key business stakeholders jointly agree and conclude that an incident should be handled as a major incident.

In the event of a major incident, senior (Management or Director) ACF personnel will take responsibility for ownership of the incident, as the Major Incident Manager, and will manage the incident to resolution as follows:

8.4. Create a Major Incident Report and complete all required entries.

8.5. Confirm the identity of the Client contact for the Major Incident, who will be responsible for all communication within the client, including Head Office, escalations and field teams.

8.6. Reviews the Major Incident report in order to ensure full understanding of the incident and all work already carried out and to formulate and manage a resolution action plan.

8.7. Obtain additional information as required from the client and any relevant third Parties.

8.8. Update the Major Incident Report (iterative steps) throughout the Major Incident lifecycle.

8.9. Set up an initial conference call with the Client contact, and any third parties, to discuss and plan the actions required. During this conference call timings for regular updates and Major Incident Report distribution should be agreed and the business impact clarified. This will all be documented in the Major Incident Report that has been raised for this occurrence.

8.10. The Major Incident Report should contain action plans and on-going root cause analysis and resolution recommendations.

8.11. Reviews/conference calls will occur at an agreed schedule to keep all parties updated with the progress of the Major Incident and plan for next actions. This will all be documented in the Major Incident Report.

8.12. Escalations required within ACF will be agreed by the Major Incident Manager and the Client contact, including any requests for additional resource if required.

8.13. Resolutions found or recommendations made are documented and discussed with all parties.

8.14. Major Incident closure is agreed if the resolution has been performed or the recommendations have been accepted by the client.

8.15. As part of the closure process a full Root Cause Analysis report (RCA) is provided to the client (part of the final Major Incident Report update). The report will be provided within 5 working days of the Major Incident being closed, unless otherwise agreed with the client

9. Incident Categorisation

P1 - Critical	P2 - High	P3 - Medium	P4 - Low	Service & Change Request
Critical: A complete Supported System, or significant component of it, is unavailable or inoperable, which prevents or is likely to prevent if not corrected, a business process from	High: Any incident which causes an adverse impact on the functionality of Q-Flow or a degraded service that impacts a business process or a total or material loss of a non-critical	Medium: A minor degradation to a component of the Supported System that does not stop any end user(s) from working	Low: Routine problem or query, which has negligible if any impact on the Supported System or ability of any end user(s) to carry on working, for example a documentation or cosmetic problem.	Service & Change Request: All ancillary and core functionality available. No disruption in existing service. Service request.

fulfilling its essential business function.	component of the Supported System where any end user(s) cannot perform any useful work on that component.			

10. Roles, Responsibilities and Escalation Levels

Role	**Responsibility**	**Escalation Level**
Support Engineer	Incident Owner	Level 1
Account Manager	Commercial Owner	Level 2
Delivery Director	Business Unit Owner	Level 3
Technical Director	Solution Owner	Level 3
Vice President, Operations and Delivery (UK Managing Director)	Business Owner	Level 4
Vice President, R&D	Product Owner	n/a

11. Response Times

ACF will respond to all incidents based on the following service levels.

Incident Category	Time to Respond	Time to Service Restoration	Time to Permanent Fix
Complete or major failure (Any incident where the Q-Flow® is substantially inoperable or unusable, or where a major function of the current release is non-functional)	1 Working Hour	Provision of a workaround or plan for resolving the incident within 4 working hours, thereafter dedicating all necessary resources to resolve the incident.	Plan for a permanent fix submitted within five (5) business days.
Urgent (Any incident which causes an adverse impact on the functionality of Q-Flow)	4 Working Hours	Provision of a workaround or plan for resolving the incident within one (1) business day, thereafter dedicating all necessary resources to resolve the incident.	Plan for a permanent fix submitted within ten (10) business days.
Routine (Cosmetic issue or minor problem which is not significantly inconveniencing to the client, or affecting business operations)	1 Business Day	Issue to be fixed within the next scheduled upgrade.	N/A

12. Internal Escalation Process

ACF will monitor all incidents, and internally escalate them based on the following service levels:

Incident Category	Update Frequency	Threshold for Escalation	Escalation Point
P1	Every 1 Hour	Immediate Immediate Immediate Immediate	Level 1 Level 2 Level 3 Level 4
P2	Every 4 Hours	Immediate 1 hours 2 hours 3 hours	Level 1 Level 2 Level 3 Level 4
P3	To be agreed when the case is logged	1 Business Day 1 Business Day 3 Business Days 4 Business Days	Level 1 Level 2 Level 3 Level 4
P4	To be agreed when the case is logged	2 Business Days 2 Business Days 3 Business Days 3 Business Days	Level 1 Level 2 Level 3 Level 4

13. Support Tiers

L1 – First Line Support:	L2 – Second Line Support	L3 – Third Line Support	L4 – Product Support
Client	**ACF ("Support Desk")**	**ACF (UK Development)**	**ACF (US / Israel Core Product Team)**
First point of call for users of the Software Receives inbound requests through channels such as phone, Web forms, email, chat, or other means, from users of the Software. Support logs, categorizes, prioritizes, tracks, and routes (i) incidents reported by users or (ii) alarms raised by monitoring tools, through to resolution.	Manages incidents raised by L1 or as agreed in documented SLA timelines. Collaborate with any other support or dependency groups in case the incident has a linkage to other support personnel or outside vendors. Escalate to L3 when documentation is insufficient to complete the tasks or do not solve the incident.	Participate in major incident management, prioritization, minor enhancements, break fix activities, problem management, stability analysis, etc. Proactively identify problems, looking for continuous service improvement opportunities. Escalate to L4 if a fix involves a major enhancement or core product development	Core product support through architects, engineers and software developers. Investigate and identify product bugs, provide detailed configuration requirements, product customisations, feature requests or other expert level guidance.

14. Client responsibilities

The client shall be responsible for first line support of the system where agreed, efforts to resolve an incident should be made prior to contacting the ACF UK service desk. In the event the incident cannot be resolved without contacting the service desk, all applicable information should be supplied before an incident can be logged and categorised for resolution.

Where the client is responsible for hardware on which the system resides, this should be maintained to a satisfactory level of maintenance and to the agreed minimum specifications on which ACF software should be used.

The client will make available resources when required in order to resolve incidents raised and will, where applicable, make available any systems via remote access or otherwise to aid the resolution of an incident.

15. Customer Satisfaction

The principle objective of the Support Desk is to ensure maximum customer satisfaction when using our services. All feedback on use of the services and the service desk itself is welcomed. Primary contact for all feedback is through your Account Manager.

Where a response is required to any feedback given, this will be managed using the same incident management processes and procedures set out in this document to facilitate a timely and satisfactory response to the client.

16. Reporting

The following data will be captured as part of ongoing service improvement practices and is able to be used for reporting to the client for the duration of their service agreement with ACF.

- Total numbers of Incidents (as a control measure)
- Breakdown of incidents at each stage (e.g. logged, work in progress, closed etc)
- Size of current incident backlog
- Number and percentage of major incidents
- Mean elapsed time to achieve incident resolution or circumvention, broken down by impact code
- Percentage of incidents handled within agreed response time as defined by SLA's or ISD standards

17. Coverage (Hours of operation)

ACF default telephone and e-mail support lines for Licensee to call for questions and technical issues regarding the Software and/or the Hardware, Monday to Friday (excluding local holidays) from 08:00 to 18:00 GMT.

18. Levels of Service

Availability. Excluding ACF Maintenance Downtime, ACF targets a minimum uptime of 95.5% (measured on a monthly basis) for the Licensed Software. ACF's hours of operation for the processing environment availability are as follows:

SERVICES	HOURS OF OPERATION
Data Centre: Systems Availability	24X7X365
Critical outage support	24x7x365

Uptime Monitoring. ACF will monitor Service delivery and report on performance and review expectations as compared to actual service and performance. Monitoring Service delivery involves tracking data including, but not limited to, issue tickets, system statistics, processing results, error logs, and environment access to poll against specified Service levels.

If contractually required, ACF will generate and distribute reports on a monthly basis to reflect Customer requirements and delivery for the prior month.

Uptime shall exclude unavailability of system caused by any of the following: A. Scheduled, announced downtime for maintenance; B. Errors, omissions, delays or failures caused by Customer, Customer employees, agents or representatives C. Force majeure events, including, without limitation, downtimes associated with the public Internet infrastructure D. Connectivity failures unrelated to ACF data center E. Inability to update your application due to failure of your provided data feeds E. Inability to connect to application due to failure of Customer workstations, site environment, network circuits or any third party network circuit engaged by customer F. Expedited or Special service requests.

Trouble Incident Response and Resolution

There are four (4) Service Request Severity Classifications: (a) Critical; (b) High; (c) Medium; and (d) Low. Critical, High and Medium Service Requests pertain to problems in the Product. Low Service Requests pertain to questions about the Product or Services. Service request can be received by either phone or email.

Critical: System down or exhibiting server errors (i.e. loss of server communication). Condition has immediate and critical impact on business. A significant number of users of the system are unable to perform their tasks as necessary. Risk of loss and customer impact is severe.

High: System degraded but working with reduced functionality. Condition impacts business. There are workarounds, however, risk of loss, customer impact or financial impact is considered serious.

Medium: Slow response time or errors, but no loss of functionality. A minor condition that has minimal impact on ability to do business. No risk of loss of customer impact.

Low: Service request or an issue with minimal business impact.

19. Hardware Support (Maintenance and Service)

19.1. Service Level Agreement: "5 Business Day" repair of, or swap-out of, faulty hardware items as listed in "Schedule of Hardware Supported".

19.2. ACF's Support and Maintenance contract will not cover any hardware equipment faults that are related to misuse or abuse. For any engineer site visits that are a result of misuse or abuse of hardware equipment, additional charges will be applied, including the cost of travel, labour and replacement hardware.

19.3. Hardware will not be supported under this or any other agreement after 3 years from date of installation. After which it is recommended that the Client purchase new hardware.

END OF EXHIBIT B

EXHIBIT C: SOFTWARE END USER LICENCE AGREEMENT

PLEASE READ THE TERMS AND CONDITIONS OF THIS END-USER LICENSE AGREEMENT (EULA) CAREFULLY BEFORE OPENING THE PACKAGE CONTAINING THE INSTALLATION COMPACT DISCS, THE COMPUTER SOFTWARE THEREIN, AND THE ACCOMPANYING USER DOCUMENTATION (TOGETHER REFERRED TO AS THE "SOFTWARE"). THE SOFTWARE IS COPYRIGHTED AND LICENSED (NOT SOLD). BY OPENING THE PACKAGE CONTAINING THE SOFTWARE, YOU ARE ACCEPTING AND AGREEING TO THE TERMS OF THIS EULA. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS EULA, YOU SHOULD PROMPTLY RETURN THE PACKAGE IN UNOPENED FORM, AND YOU WILL RECEIVE A REFUND OF YOUR MONEY. THIS EULA REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE SOFTWARE BETWEEN YOU AND ACF INC. (REFERRED TO AS "LICENSOR"), AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES.

1. License Grant.

Licensor hereby grants to you, and you accept, a nonexclusive license to use the software known as Q-Flow®, including machine-readable program code stored on CD-ROM, any future updates or upgrades (new versions or releases which may be offered by the Licensor to End – User from time to time), manuals and accompanying documentation contained therein (collectively referred to as the "Software"), only as authorized in this EULA. The Software may be used only on computers owned, leased, or otherwise controlled by you; or in the event of the inoperability of that computer, on a backup computer selected by you. Neither concurrent use on two or more computers nor use in a local area network or other network is permitted without separate authorization and the payment of other license fees. You agree that you will not assign, sublicense, transfer, pledge, lease, rent, or share your rights under this EULA. You agree that you may not reverse assemble, reverse compile, or otherwise translate the Software. Upon loading the Software into your computer, you may retain the compact discs for backup purposes. In addition, you may make one copy of the Software on a second set of discs (or on cassette tape) for the purpose of backup in the event the Software diskettes are damaged or destroyed. You may make one copy of the accompanying documentation including the attached User's Manual for backup purposes. Any such copies of the Software shall include Licensor's copyright and other proprietary notices. Except as authorized under this paragraph, no copies of the Software or any portions thereof may be made by you or any person under your authority or control.

2. Maintenance and Support Services.

You may be provided with technical maintenance and support services related to the Software that may include assistance in the installation and integration of the Software, consulting, on-site support, on – line technical support during normal business hours

("Services"), by the Licensor or a third party upon signature of a separate agreement ("Support and Maintenance Agreement"), and the payment of fees as therein specified. During the first 1 year of the Warranty Period, as defined hereunder, the Services shall be granted for free. Any supplemental software code provided to you as part of the Services shall be considered as part of the Software and be subject to the terms of this EULA. With respect to technical information you provide to the provider of the Services as part of the Services, Licensor may use such information for its business purposes, including for product support and development. Licensor will not utilize such technical information in a form that personally identifies you except to the extent necessary to provide you with the Services.

3. Replacement, Modification and Upgrade of the Software.

Licensor may offer you, either personally or through a third party, to replace, modify or upgrade the Software at any time by offering you a replacement or a modified, updated or upgraded version of the Software (the "New Version") and to charge you for a New Version , should you accept such offer. Any such replacements or modified software codes or upgrades to the Software shall be governed by the Support Agreement. Any such replacements or modified software codes or upgrades to the Software offered to you by Licensor shall be considered part of the Software and subject to the terms of this EULA (unless this EULA is superseded by a further EULA accompanying such replacement or modified version of or upgrade to the Software). In the event that Licensor offers a replacement or modified version of or any upgrade to the Software, (a) your continued use of the Software is conditioned on your acceptance of such replacement or modified version of or upgrade to the Software and any accompanying superseding EULA and (b) in the case of the replacement or modified Software, your use of all prior versions of the Software is terminated. Refraining from accepting the New Version might cause an immediate termination of the Support Agreement and the Warranty as defined hereunder, according to Licensor's sole discretion.

4. Licensor's Rights.

You acknowledge and agree that the Software is a proprietary product of Licensor protected under U.S. copyright law. You further acknowledge and agree that all right, title, and interest in and to the Software, including associated intellectual property rights, are and shall remain with Licensor. This EULA does not convey to you an interest in or to the Software, but only a limited right of use revocable in accordance with the terms of this EULA.

5. License Fees.

The license fees paid by you are paid in consideration of the license(s) granted under this EULA.

6. Term.

This EULA is effective upon your opening of this package and shall continue indefinitely, except if terminated according to the terms of this EULA. You may terminate this EULA at any time by returning the Software and all copies thereof and extracts there from to Licensor. In addition to any other right to terminate, and without prejudice to any other rights, Licensor may terminate this EULA if you fail to comply with the terms and conditions of this EULA. Licensor may terminate this EULA by offering you a superseding EULA for the Software or a New Version conditioning your continued use of the Software or such a New Version on your acceptance of such superseding EULA. Upon termination, you agree to return to Licensor the Software and all copies and portions thereof.

7. Limited Warranty.

Licensor warrants, for your benefit alone, that the software is distributed and licensed in accordance with the published documentation, and that for a period of 12 months from the date of the commencement of this EULA (referred to as the "Warranty Period") the diskettes in which the Software is contained are free from defects in material and workmanship. Licensor further warrants, for your benefit alone, that during the Warranty Period the Software shall operate substantially in accordance with the functional specifications in the User's Manual. If during the Warranty Period, a defect in the Software appears, you may return the Software to Licensor for either repair, or replacement of the Software in case of a defect which results in a complete failure to install or operate it, if so elected by Licensor provided, however, that Licensor shall be relieved from any obligations under this Limited Warranty if you do not give Licensor prompt written notice of any defect claimed hereunder and if such delay causes additional degradation of the Software. You agree that the foregoing constitutes your sole and exclusive remedy from Licensor regarding the Software. All of the warranties made by Licensor hereunder are, and all obligations of Licensor under this EULA shall be, contingent upon your use of the Software in accordance with the Users' Manual and specific instructions relating thereto furnished by Licensor and, to the extent that any of the following cause warranty failure, no such warranties or obligations shall apply to any portion of the Software that has been:

7.1. Installed or operated by you and/or any third party in a manner inconsistent with the provisions of this EULA and/or the Users' Manual or modified by a party other than Licensor without the written approval of Licensor; or

7.2. Damaged by negligence or misuse by other than Licensor or by fire, casualty, or other external causes; or

7.3. Subjected to conditions beyond the environmental and operating constraints specified in the Users' Manual attached hereto, or subjected by parties other than Licensor to unusual physical or electrical stress; or

7.4. Installed or operated by you and/or by a third party on inappropriate hardware programs not consistent with the Licensor's instructions regarding the type of hardware to be used with the Software; or

7.5. Operated without having a license to do so.

The Company does not in any way warrant that Software functions will meet your specific requirements, or that the operation of the Software will be uninterrupted, error-free, secured, supplied immediately on request, produce accurate and reliable results and contain true and correct information. Due to the complex nature of computer programs, the Software (like all large programs) will probably never be completely error-free.

EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE SOFTWARE CONTAINED THEREIN, IS LICENSED "AS IS," AND LICENSOR DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

8. Warranty of Right to License; Non infringement.

Licensor warrants that it is the sole owner of the Software, that it has the right to convey the licenses set forth herein, and that your use of such Software in accordance with the terms of this EULA shall not infringe any third-party rights in copyright or trade secret in the United States.

9. Additional Limitation of Liability.

Licensor's cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this Agreement shall not exceed the license fee paid to Licensor for the use of the Software. In no event shall Licensor be liable for any indirect, incidental, consequential, special, or exemplary damages or lost profits, due to negligence on the part of the Licensor or any distributor, reseller or dealer, even if Licensor has been advised of the possibility of such damages.

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

10. Trademark.

Q-Flow® is a registered trademark of Licensor. No right, license, or interest to such trademark is granted hereunder, and you agree that no such right, license, or interest shall be asserted by you with respect to such trademark.

11. Governing Law.

This EULA shall be construed and governed in accordance with the laws of the State of New York.

12. Costs of Litigation.

If any action is brought by either party to this EULA against the other party regarding the subject matter hereof, the prevailing party shall be entitled to recover, in addition to any other relief granted, reasonable attorney fees and expenses of litigation.

13. Severability.

Should any term of this EULA be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof.

14. No Waiver.

The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

15. U.S. Government Restricted Rights.

The Software and related documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 C.F.R. 52.227-19, as applicable. Manufacturer for such purpose is Q-nomy Inc, SunTrust International Center, SE 3rd Ave suite 1410, Miami, FL 33131, USA.

END OF EXHIBIT C

EXHIBIT D: MUTUAL NON-DISCLOSURE AGREEMENT

1. Definitions

1.1. "**Confidential Information**" shall mean Information of a confidential nature which relates to the business, products or services of either of the parties (whether written, visual or oral) including, without limitation, technical know-how, trade secrets, technical data, analyses, compilations, concepts, technical processes, formulae, specifications, inventions, research projects, customer and supplier lists, information regarding customer types and categories and the geographical area of operation of customers, pricing policies, operational methods, financial information, marketing information and other significant business information of that party, its subsidiaries and shareholders.

1.2. "**Disclosing Party**" shall mean the party which discloses Confidential Information to the other. party

1.3. "**Purpose**" shall mean for the provision of information relating to provision of Hardware, Software or Services relating to Customer Queuing, Flow Management, Ticketing and Customer Experience solutions.

1.4. "**Receiving Party**" shall mean the party receiving the Confidential Information.

1.5. "**Representatives**" shall mean advisors, employees, directors, agents or representatives of a party, including those of members of the group of companies of which a party is a member.

2. Use of Confidential Information

The Receiving Party agrees and undertakes that:

2.1. it will hold all Confidential Information received from a Disclosing Party in strict confidence;

2.2. it will only use the Confidential Information in connection with the Purpose; and

2.3. it will only copy, reproduce, or reduce to writing any part of the Confidential Information to the extent that it is reasonably necessary for the Purpose;

2.4. it will only disclose the Confidential Information to such of its Representatives who need to know the same for the Purpose and provided that:

2.4.1. the Representatives are made aware of the provisions of this Agreement and are required to keep such information confidential;

2.4.2. the Receiving Party will be liable for any breach of the terms of this Agreement by any of its Representatives; and

2.4.3. security measures will be applied to protect the Confidential Information which are at least equivalent to those applied by the Receiving Party to its own confidential or proprietary information.

2.5. it will comply fully with current Data Protection legislation.

2.6. All documents containing Confidential Information supplied by the Disclosing Party, and electronic copies thereof in whatever form, shall (as determined by the Receiving Party) be either destroyed or returned by the Receiving Party within 10 days of written request from the Disclosing Party; provided always that:

2.6.1. each Party's professional advisers may continue to hold one copy of the Confidential Information to support professional advice given by them in connection with the Purpose or to comply with their professional duties, in each case, subject to the terms of this Agreement; and

2.6.2. the portion of the Confidential Information which consists of or is incorporated (either fully or partially) into analyses, compilations, studies or other documents prepared by either Party or its Representatives may be retained by that Party, subject in each case to the terms of this Agreement.

3. Exclusions

The obligations of confidentiality shall not apply to any part the Confidential Information which:

3.1. is already known to the Receiving Party at the time of disclosure (as evidenced by its written records) or is independently developed by the Receiving Party without access to, or use or knowledge of, the Confidential Information of the Disclosing Party;

3.2. is approved for release by the Disclosing Party;

3.3. becomes publicly known through no fault of the Receiving Party or its Representatives;

3.4. is disclosed to the Receiving Party by a third party who is not subject to any confidentiality obligations; or

3.5. the Receiving Party is required by law or by any administrative, governmental or regulatory authority to disclose, provided that where practicable it gives the Disclosing Party advance notice of such disclosure in order to enable the Disclosing Party to take action to prevent such disclosure.

4. Period of Agreement

This Agreement shall terminate upon the mutual agreement of the parties, or upon the signature of an agreement by both parties containing provisions which are expressed to replace the confidentiality provisions of this Agreement. If the proposed transaction is not completed or does not take place, the undertakings contained in this letter will continue in full force and effect for a period of three years from the date of disclosure of any Confidential Information.

5. General

5.1. No announcement concerning the existence of this Agreement or the Purpose, or any matter ancillary thereto, shall be made by either party except with the written consent of the other party or where required by law or the rules of any governmental, administrative or regulatory authority.

5.2. Each party reserves all rights in its Confidential Information. No license or conveyance of any rights to either Party in respect of any discoveries, inventions or patents is granted or implied by this Agreement or by the transmission of Confidential Information between the Parties.

5.3. Neither party makes any representations or warranties in respect of the Confidential Information provided to the other party.

5.4. The supply of Confidential Information shall not be taken as any form of commitment on the part of either party to proceed with any transaction.

5.5. Following signature of this Agreement and for a period of 12 months following the earlier of (a) the date on which negotiations between the parties irretrievably breakdown and (b) completion of the Purpose, neither party shall, directly or indirectly, solicit for employment any employee of the other party save through a general recruitment campaign made in the trade or other press.

5.6. Neither party may without the written consent of the other assign any of the benefits or obligations of this Agreement to any third party

5.7. This Agreement shall be governed by and construed in accordance with English law and each party agrees to submit to the jurisdiction of the English Courts as regards any claim or matter arising under this Agreement.

5.8. In the event that any of the provisions of this Agreement is held to be legally invalid or unenforceable, it shall not affect the validity of the remaining provisions hereof which shall continue in full force and effect between the parties hereto.

5.9. All notices hereunder shall be in writing addressed to the parties at their respective addresses set forth in this Agreement, or such other address as may be notified from time to time by either party to the other.

5.10. A person who is not a party to this Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement but this does not affect any right or remedy of a third party which exists or is available apart from that Act.

EXHIBIT A: FEES

7. Indicative Cost Breakdown prepared by ACF

Six Month Cost	[redacted]
Software	
Address Look-Up*	
Hosting	
Support	
Professional Services**	
Ongoing Quarterly Cos	
Software	
Hosting	
Support	

*Address look-ups are initially charged at [redacted] it is currently unknown when this threshold will be hit. The ongoing costs for this service is [redacted], ACF will report regularly to manage expectations, and additional requirements invoice monthly.

**ACF have provided the initial 10 days free of charge - further days are charged at our standard rate and invoiced monthly. It is currently estimated that to deliver the tactical MVP phase, this will consume the remaining days of the first 10 FOC (currently 3 days remaining), plus an additional 10 that would be chargeable. The remaining 30 are for your budgetary purposes as we expect some level of change after the initial go live and ongoing change management/ requests that may occur in the first 6 months.

***The scope of requirement for future phases is unknown, therefore we are unable to estimate the professional services required past the first six months, these will be charged at our daily rate and invoiced monthly.

- END OF DOCUMENT –

DATA PROCESSING AGREEMENT

Dated

11th April 2020

BETWEEN

The Secretary of State for Health and Social Care

the "Client"

and

ACF Technologies (UK) Ltd

DATA PROCESSING AGREEMENT dated: 11th April 2020

BETWEEN:

(1) **The Secretary of State for Health and Social Care acting as part of the Crown through the Department of Health and Social Care**, whose registered office is at 39 Victoria Street, Westminster, London SW1H 0EU (**"Controller" or "Client" or "Customer"**); and

(2) **ACF Technologies UK Ltd** (company number 6460227) whose registered office is at TECHNOLOGY HOUSE, 48-54 GOLDSWORTH ROAD, WOKING, SURREY, GU21 6LE (the "Provider" and/or the "Supplier") ("**Processor" or "Provider"**)

RECITALS

(A) Controller and Processor have entered into a services agreement on 11th April 2020 pursuant to which Processor will perform the Services (as defined below) (the "**Services Agreement**").

(B) In order to perform the Services, Processor will need to process certain Personal Data (as defined below) on behalf of Controller.

(C) The parties now wish to enter into this Agreement in order to regulate the provision and use of the Personal Data by Processor.

1. **DEFINITIONS AND INTERPRETATION**

1.1 The following words and phrases used in this Agreement and the Schedules shall have the following meanings except where the context otherwise requires:

"Adequate Jurisdiction"	means a jurisdiction outside the European Economic Area that has been determined to have in place adequate data protection laws, pursuant to a valid Decision Notice issued by the European Commission;
"Affiliate"	means in relation to a company, any subsidiary, subsidiary undertaking and holding company of the company (as those terms are

defined in sections 1159 and 1162 of the Companies Act 2006), any subsidiary and subsidiary undertaking of such holding company. A company shall be treated, for the purposes only of the membership requirement contained in subsections 1159(1) (b) and (c), as a member of another company even if its shares in that other company are registered in the name of (a) another person (or its nominee) by way of security or in connection with the taking of security, or (b) its nominee, and shall include a body corporate outside the UK. In the case of a limited liability partnership which is a subsidiary of a company or another limited liability partnership, section 1159 of the Companies Act 2006 shall be amended so that: (a) references in sub sections 1159(1)(a) and (c) to voting rights are to the members' rights to vote on all or substantially all matters which are decided by a vote of the members of the limited liability partnership; and (b) the reference in section 1159(1)(b) to the right to appoint or remove a majority of its board of directors is to the right to appoint or remove members holding a majority of the voting rights.

"Confidential Information" means all information relating to Controller's customers and prospective customers (including without limitation the Personal Data), current and projected financial or trading situations, business plans, business strategies, developments and all other information relating to Controller's business affairs including all other information of a confidential nature imparted by Controller to Processor during the term of this Agreement or coming into existence as a result of

Processor's obligations;

"Data Protection Laws" means the General Data Protection Regulation (EU) 2016/679, the Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (and all applicable laws which replace it, including the e– Privacy Regulation) and all applicable Laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner (or the data protection authority which replaces it).

Any reference in this Agreement to "data controller", "data processor", "data subjects", "personal data", "process", "processed", "processing" and "supervisor authority" shall have the meaning set out in, and will be interpreted in accordance with:

a) in respect of processing undertaken on or after 25 May 2018, the General Data Protection Regulation (EU) 2016/679 and the Data Protection Act 2018; and
b) in respect of processing undertaken on or after the date on which legislation comes into force that, in respect of the United Kingdom, replaces the General Data Protection Regulation (EU) 2016/679 and the Data Protection Act 2018, that legislation.

"Personal Data" means personal data (as defined under the definition of "Data Protection Laws")

processed by the Provider pursuant to the terms of this Agreement, including (without limitation) that which is described in Schedule 1;

"Regulators" means (as the case may be) the Financial Conduct Authority, the Prudential Regulation Authority, the Bank of England, the Information Commissioner Office and/or such other governmental, regulatory or selfregulatory bodies as Provider or Client may from time to time be subject.

"Services" means the services to be carried out by Processor on behalf of Controller, pursuant the Services Agreement; and

"**Standard Contractual Clauses**" means the EU standard contractual clauses for Data Processors established in third countries pursuant to European Commission Decision (2010/87/EU) of 5 February 2010 under the EU Directive (95/46/EC), as amended from time to time.

1.2 The headings in this Agreement are inserted for convenience only and shall not affect its construction or interpretation.

1.3 References in this Agreement to Clauses and Schedules are, unless otherwise stated, references to the clauses of and schedules of this Agreement.

1.4 Except where the context otherwise requires, the masculine includes the feminine, the singular includes the plural and, in each case, vice versa;

1.5 Unless otherwise stated, references to a statute or any section of any statute include any statutory amendment, modification or re-enactment and instruments and regulations under it in force from time to time; references to regulatory rules include any amendments or revisions to such rules from time to time; references to regulatory authorities refer to any successor regulatory authorities.

3. **THE TERM**

With effect from the 11th April 2020.

This Agreement shall continue in full force unless or until terminated by either party giving to the other three month's written notice to expire at any time or unless terminated for breach by either party in accordance with clause 9.

4. **OBLIGATIONS OF CONTROLLER**

To the extent permitted by the Data Protection Laws, Controller shall provide the Personal Data to Processor together with such other information as Processor may reasonably require in order for Processor to provide the Services.

5. **OBLIGATIONS OF PROCESSOR**

5.1 For the purposes of Services provided by Processor under this Agreement and the Services Agreement, the Controller authorises the Processor to process the Personal Data on its behalf and the parties agree that the Controller (and/or the relevant Controller Affiliate) is the data controller and the Processor shall be the data processor in relation to the Personal Data, and when acting in its capacity as a data processor, the Processor shall (and will ensure that all authorised Sub-processors shall) at all times, process Personal Data in accordance with its obligations under the Data Protection Laws and:

(a) process Personal Data only to the extent necessary to provide the Services and only in accordance with documented instructions from Controller (including with regard to transfers to a third country or an international organisation). This section shall apply unless the Processor is required to process Personal Data otherwise than as instructed, in accordance with European Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law also prohibits such information on important grounds of public interest;

(b) immediately inform the Controller if, in its reasonable opinion, an instruction received in connection with this clause 5 infringes any Data Protection Laws;

(c) ensure that persons authorized to process the Personal Data accesses such Personal Data strictly on a need to know basis as necessary to perform their roles in the provision of the Services[, have received training

in relation to their obligations regarding the handling of Personal Data, pursuant to this Agreement and the Data Protection Laws, and have committed themselves to confidentiality obligations no less stringent than the confidentiality obligations imposed on the Processor under this Agreement or are under an appropriate statutory obligation of confidentiality;

(d) subject to clauses 5.1 (e) and (f), not use subcontractors, Affiliates of Processor or any other third party to process Personal Data ("**Subprocessors**") under this Agreement unless it has obtained the prior, written consent from the Controller to do so and provided at all times that the Processor has entered into a written contract with such Subprocessor, which includes the same obligations on the Sub-processor as those imposed on the Processor by the Controller under this Agreement, prior to any processing of the Personal Data by the Subprocessor taking place;

(e) subject to clauses 5.1 (d) and (f), not process Personal Data (and shall ensure that no third party processes Personal Data) outside of the European Economic Area ("**EEA**") without having first obtained Customer's prior written consent, which may be given at the discretion of the Controller and only provided that either:

a. the Standard Contractual Clauses are entered into between the Controller (or relevant Controller Affiliate) as '*data exporter*' and the relevant recipient of the Personal Data as '*data importer*' prior to such transfer taking place; or
b. the transfer is to a recipient located within an Adequate Jurisdiction (subject to any applicable restrictions); or
c. such other valid and adequate transfer mechanisms as approved by the European Commission, have been or will be put in place, as agreed between the Controller and the Processor, prior to the transfer taking place, and

in the event that any of the above transfer mechanisms should be held to be invalid, the Processor shall (at the discretion of the Customer), either put in place, within the transition period prescribed by the relevant Regulator, such alternative valid adequate transfer mechanisms as approved by the Controller or, if unable to do so, cease the transfer of affected Personal Data at the end of the aforementioned transition period;

(f) where permitted to use Sub-processors and/or (respectively) transfer Personal Data outside the EEA under the preceding subsections (d) and/or (e), the Processor will maintain a record (as set out in subsection (h) below) of the relevant Sub-processors and/or (respectively) countries and entities to which Personal data has been transferred andshall remain fully liable for any act(s) and/or omission(s) of any Sub-processors engaged pursuant to this Agreement that constitute breach of the data protection requirements imposed on the Processor under this Agreement as if these acts and/or omissions were Processor's own acts and/or omissions;

(g) implement appropriate technical and organisational measures to ensure **a level of security appropriate to the risk** presented by processing the Personal Data, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed in accordance with the Data Protection Laws, including as a minimum the measures required pursuant to the Security Schedule (attached to this Agreement as Schedule 2) and, as appropriate;

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing;

(h) maintain a written record, including in electronic form (the "**Data Record**"), of all categories of processing activities carried out on behalf of the Controller and promptly upon request provide a copy of the Data Record to the Customer, which shall contain the following details:

a. the name and the contact details of the Processor and (where applicable) its Sub-processors acting on its behalf and details of their respective data protection officer (as applicable);

b. the categories of personal data, data subjects and processing activities carried out on behalf of the Customer;
c. where applicable, transfers of personal data to a third country (i.e. non EU Member State) or an international organisation, including identification of that third country or international organisation and documentation evidencing implementation of suitable safeguards; and
d. a general description of the technical and organisational security measures referred to Article 32(1) of the GDPR;

(i) notify the Controller in writing and without undue delay (and in any event, not later than 24 hours) after becoming aware of a reasonably suspected, "near miss" or actual breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by the Processor (or any Sub-processor) under this Agreement (a "**Data Security Incident**"), including the nature of the Data Security Incident, the categories and approximate number of data subjects and Personal Data records concerned and any measure proposed to be taken to address the Data Security Incident and to mitigate its possible adverse effects, and where, and in so far as, it is not possible to provide all the relevant information at the same time, the information may be provided in phases without undue further delay, but the Processor (and Sub-processor, as applicable) may not delay notification under this clause 5 (i) on the basis that an investigation is incomplete or ongoing;

(j) will not, and will procure that Sub-processors will not, make or permit any announcement, public disclosure or regulatory notification in respect of the Data Security Incident to any person without the Customer's prior written consent, which may be given, withheld or made subject to conditions at the Customer's sole discretion;

(k) provide, upon request from the Controller or a supervisory authority, all reasonable cooperation and assistance to the Controller in order to facilitate the Controller in complying with its obligations under Data Protection Laws and/or for the purposes of cooperating and/or liaising with the supervisory authorities;

(l) provide reasonable assistance to the Controller in:

a. responding to requests for exercising data subjects' rights under the Data Protection Laws, including by notifying the Controller without delay of any such request the Processor may receive from a data subject in respect of the processing of their Personal Data;

b. responding to communications received from Regulators or supervisory authorities (including the Information Commissioner's Office) in respect of the processing of Personal Data under this Agreement, including by notifying the Controller without delay of any such communication the Processor may receive from a Regulator, unless the Processor is prohibited from notifying the Controller pursuant to applicable laws;

c. documenting any Data Security Incidents and reporting any Data Security Incidents to any Regulator or supervisory authority and/or data subjects;

d. taking measures to address Data Security Incidents, including, where appropriate, measures to mitigate their possible adverse effects;

e. conducting data privacy impact assessments of any processing operations in relation to the Personal Data, and consulting with any applicable Regulator or supervisory authority or appropriate persons, accordingly; and

f. promptly upon request of the Customer, transferring Personal Data to a third party in compliance with a request from a Data Subject to exercise their right to data portability

(m) make available to the Controller all information necessary to demonstrate compliance with the obligations set out in this clause 5.1, and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

5.2 Subject to clause 5.4, following a request from the Controller., the Processor shall (at the Controller's discretion) promptly return or delete (or destroy) all Personal Data held by the Processor (or Sub-processor) and certify (within 14 days of such request) that this clause 5.2 has been complied with.

5.3 Where no specific request has been placed by the Controller under clause 5.2 above and subject to clause 5.4, within a period of six (6) months following termination of this

Agreement, the Processor will (and will ensure that all Sub-processors will) securely delete or destroy all copies of Personal Data held by the Processor (or Subprocessor), and certify that Personal Data has been deleted or destroyed, provided that it gives at least 30 days' notice to the Controller of when such deletion or destruction is to occur, giving the Controller an opportunity to object or provide alternative instructions in accordance with clause 5.2.

5.4 Where the Processor (or Sub-processor) is required to retain Personal Data in order to comply with applicable laws, the Processor must notify the Controller and shall retain such Personal Data only in its capacity as a data controller and shall comply with its obligations as a data controller pursuant to the Data Protection Laws.

6. INDEMNITY

Processor agrees to indemnify Controller against any and all losses, costs, expenses (including legal expenses), damages, liabilities, demands, claims, fines, actions or proceedings (including reasonable legal costs, fines and claims for damages) which Controller and or its Affiliates may suffer or incur as a consequence of the Processor's breach of clauses 5 and 8.

7. OWNERSHIP

All right, title and interest in the Confidential Information shall vest solely in Controller.

8. CONFIDENTIALITY

8.1 Processor shall procure that all Confidential Information disclosed to it by Controller under this Agreement or which at any time during the term come into Processor's knowledge, possession or control (including all outputs or adaptations of Confidential Information which result from Services provided under this Agreement), shall be kept secret and confidential and shall not be used for any purposes other than those required or permitted by this Agreement and shall not be disclosed to any third party except insofar as this may be required for the proper operation of this Agreement and then only under appropriate confidentiality provisions approved by Controller.

8.2 Processor shall promptly notify Controller if any Confidential Information is required by law to be disclosed by it or any other person receiving it under or pursuant to this Agreement and shall co-operate with Controller regarding the manner of such disclosure (but without

prejudice to any obligation to comply with any law). The obligations of confidentiality shall not apply to any information which:

8.2.1 is or becomes generally known to third parties (other than as a result of a breach of the provisions of this Agreement); or

8.2.2 which is already lawfully in, or which comes lawfully into, Processor's possession other than under this Agreement; or

8.2.3 is independently developed by Processor.

8.3 To the extent that there is any conflict between the terms of this clause 8 and the terms of clause 5, the terms of clause 5 shall prevail.

9. **TERMINATION**

This Agreement may be terminated with immediate effect by either party giving written notice to the other where:

9.1 the Services Agreement is terminated;

9.2 the other party is in breach of any material obligation under this Agreement and, where the breach is capable of remedy, has failed to remedy the breach within 21 days of receipt of notice so to do; or

9.3 a resolution is passed or an order is made for the winding up of the other party (otherwise than for the purposes of solvent amalgamation or reconstruction) or an administrator, a receiver or an administrative receiver is appointed or an encumbrancer takes possession of any of the other party's property or assets or if the other party is dissolved; or

9.4 the other party ceases or threatens to cease to carry on business in its jurisdiction of incorporation.

10. **CONSEQUENCES OF TERMINATION**

Subject to clauses 5.2, 5.3 and 5.4, on termination of this Agreement for whatever reason, Processor shall cease to use the Confidential Information and shall arrange for the prompt and safe return of all Confidential Information belonging to Controller together with all

copies of the Confidential Information in its possession or control or in the possession or control of its agents or contractors.

11. **NOTICES**

Any notice under or in connection with this Agreement shall be in writing (but not by fax, email or other electronic means) and shall be delivered personally, or sent by courier or by recorded or registered mail to the following addresses:

Notices to the Processor:

Address:	Technology House, 48-54 Goldsworth Road, Woking, Surrey GU21 6LE
Marked for the attention of:	[redacted]

Notices to Controller:

Address:	Department of Health and Social Care, 39 Victoria Street, Westminster, London, SW1H 0EU
Marked for the attention of:	[redacted]
With copies to:	N/A
Address:	N/A

A notice shall become effective on the date it is delivered to the address of the recipient party shown above. A party may notify the other of a change to its notice details.

12. **INVALIDITY**

12.1 If any provision of this Agreement is found by any court or administrative body of competent jurisdiction to be invalid, illegal or unenforceable in any respect under the law of any jurisdiction:

12.1.1 the validity, legality and enforceability under the law of that jurisdiction of any other provisions; and

12.1.2 the validity, legality and enforceability under the law of any other jurisdiction of that or any other provision,

shall not be affected or impaired in any way thereby.

12.2 If any provision of this Agreement shall be held to be void or declared illegal, invalid or unenforceable for any reason whatsoever, such provision shall be divisible from this Agreement and shall be deemed to be deleted from this Agreement and the validity of the remaining provisions shall not be affected.

13. ENTIRE AGREEMENT

This Agreement (including the Schedules) together with the Services Agreement, contains the entire and exclusive agreement and understanding between the parties on the subject matter contained in this Agreement and the Services Agreement and supersedes all related prior agreements, understandings and arrangements. The parties therefore agree that:

13.1 no representation, assurance, warranty, undertaking or promise shall be deemed to have been given or implied from anything said or written in negotiations between the parties prior to this Agreement and the Services Agreement; and

13.2 each party warrants that, in entering into this Agreement and the Services Agreement, it has not relied on any representation, assurance, warranty, undertaking or promise of any person.

Nothing in this clause shall limit or exclude a party's liability for fraud, fraudulent misrepresentation or fraudulent concealment.

14. NO WAIVER

14.1 A waiver of any term, provision or condition of, or consent granted under, this Agreement shall be effective only if expressly stated to be a waiver and communicated to the other party in accordance with the provisions of clause 11 and then only in the instance and for the purpose for which it is given.

14.2 A waiver by either party of a breach of contract or any obligation of the other party does not constitute a waiver of any future or other obligation of the said party.

14.3 No failure or delay on the part of any party in exercising any right, power or privilege under this Agreement shall operate as a waiver, nor shall any single or partial exercise of any such

right, power or privilege preclude its further exercise or the exercise of any other right, power or privilege.

14.4 Except as expressly stated in this Agreement, no right or remedy conferred upon any party by this Agreement shall be exclusive of any other right or remedy howsoever arising and all such rights and remedies shall be cumulative.

15. GOVERNING LAW AND JURISDICTION

15.1 This Agreement (and any dispute, controversy, proceedings or claim of whatever nature arising out of or in any way relating to this Agreement, its termination or its formation) shall be governed by and construed in accordance with the laws of England and Wales.

15.2 Each party agrees to submit to the exclusive jurisdiction of the courts of England and Wales.

16 COUNTERPARTS

This Agreement may be entered into in any number of counterparts by the parties to it and on separate counterparts each of which when so executed and delivered shall be an original but all such counterparts together shall constitute one and the same instrument.

IN WITNESS duly authorised executives of the parties have signed this Agreement the day and year first above written

SIGNED for and on behalf of Processor

Signed [redacted]

Title [redacted]

Date 11th April 2020

SIGNED for and on behalf of Controller

Signed [redacted]

Title [redacted]

Date DHSC _____

SCHEDULE 1
PERSONAL DATA

Data subjects

The Personal Data Processed concern the following categories of Data Subjects:

- ✓ Employees, agents and staff of [Controller] and/or [Controller Affiliate] ("**Employees**");
- ✓ Individual customers of [Controller] and/or [Controller Affiliate] ("**Customers**");

Categories of data

The Personal Data Processed concern the following categories of Personal Data:

In relation to Employees:

- ✓ Name;
- ✓ Contact details (including postal address, email address and telephone number);

In relation to Customers:

- ✓ Name;
- ✓ Contact details (including postal address, email address and telephone number);

Processing operations

The Personal Data will be subject to the following basic Processing activities:

In relation to the **categories of Employee Personal Data**, described above:

- To facilitate booking of appointments for customers with named individuals at The Client

In relation to the **categories of Customer Personal Data**, described above:

- To enable appointments to be booked with a minimum level of customer information supplied to enable a valuable appointment and a personalised service

The duration of the Processing

The above Personal Data will be processed in connection with the Services for the duration of the Agreement, such shorter period where the Processing is no longer authorised and in respect of any post-termination processing activities permitted by the Controller from time to time.

SCHEDULE 2 SECURITY SCHEDULE

For the purposes of this Schedule only, the following defined terms shall have the following meanings and all other defined terms in this Schedule shall have the meaning given in the Agreement:

"Client"	Means the Controller as defined in the Agreement.
"Confidential Information"	Means any and all written, electronic and oral information disclosed by Client to the Provider pursuant to, or otherwise in connection with, this Agreement, including, without limitation, information relating to the Client's products, services, clients, providers, operations, processes, plans or intentions, know-how, intellectual property, market opportunities and business affairs whether in writing, orally or by any another means and whether directly or indirectly (including by Client's Affiliates, contractors and/or third parties).
"Information Security Management System"	Means the framework of policies and procedures that include all legal, physical and technical controls involved in an organisation's information's information risk management processes as defined by ISO/IEC 27001 or any subsequently adopted industry standard.
"**Information Security Questionnaire**"	Means The Client's annual information security governance compliance measurement questionnaire.
"**Logical Access**"	Means the method of gaining electronic access into the System including but not limited to user accounts, vendor accounts and service accounts.
"Near Miss"	Means a Security Incident that had the potential but did not result in the materialisation of financial or non-financial impacts due to fortuitous conditions, circumstances and interventions.
"**Physical Access**"	Means the method of gaining physical access to the Premises.
"**Portable Computing Device**"	Means any item of equipment used to collect, process, store, transmit or access information whose design renders the item portable. Such items shall include but not be limited to laptop computers, USB storage devices, external hard disk units and handheld computers.
"**Portable Media**"	Means any medium which can be used to store information whose design renders the item portable. Such items shall include but not be limited to CDs, DVDs and tapes.
"**Premises**"	Means those parts of the parties' respective premises upon which the Services will be performed or received and/or as

	may be listed in the main body and/or the associated Schedules of the Agreement.
"Provider"	Means the Processor as defined in this Agreement
"**The Client Data**"	Means information provided by or on behalf of the Client or any Client Affiliate to the Provider or any of its Affiliates, pursuant to the Agreement, including (without limitation) Confidential Data and Personal Data.
"**Security Incident**"	Means (i) unauthorised Physical Access and/or Logical Access and/or (ii) a breach of the Security Policies and Standards whether through or by reason of accident, negligence or wilful default, potentially or actually causing a compromise to The Client Data from the perspectives of confidentiality, integrity and/or availability.
"System"	Means the electronic system which can consist of a single or collection of electronic assets (namely but not limited to operating systems, application software, application programming interfaces (API), databases, system routines, file transfer processes, storage, computer and network hardware devices) used to collect, process, store or transmit The Client Data and any associated electronic and nonelectronic methods, processes, procedures, routines, input and output.

For the avoidance of doubt, when/where The Client Data includes Personal Data and there is a conflict and/or inconsistency between the provisions of this Security Schedule and provisions contained elsewhere within the Agreement (including, in particular, but not limited to Personal Data processing provisions) which impose stricter obligations on the Provider in relation to processing of Personal Data, the latter provisions shall prevail.

The Provider shall implement and maintain a comprehensive security policy ("**Security Policy**") that satisfies the requirements set forth below:

1. General

The Provider shall ensure that an effective Information Security Management System is implemented, consistent with the principles of ISO/IEC 27001, having relevant and adequate coverage of the following areas:

- Security policy management;
- Corporate security management;
- Organizational asset management;
- Human resource security management
- Physical and environmental security management
- Communications and operations management
- Information access control management
- Information systems security management
- Information security incident management
- Business continuity management
- Compliance management

All applicable regulations, legal requirements and industry standards (including but not limited to SSAE 16 – SOC2, PCI—DSS and Cloud Security Alliance (CSA) where relevant and appropriate) must be reflected and specified by the Provider in the Security Policy and Information Security Management System.

The Provider shall implement and comply with DMARC (Domain-based Message Authentication, Reporting and Conformance) when sending emails on behalf of the Client. The Provider's DMARC policy (also known as the message disposition) must stipulate "reject" for all domains used to communicate with parties on the Client's behalf.

2. Risk Assessment

The Provider shall perform regular (and in any event no less frequently than at every twelve (12) month intervals) risk assessments ("**Risk Assessments**") in order to:

- identify reasonably foreseeable threats that could result in unauthorised access, copying, use, process, disclosure, alteration, transfer, unavailability, loss or destruction of any The Client Data;
- assess the likelihood of these threats occurring, and the potential damage that might result, financial and non-financial, taking into consideration the nature and classification of The Client Data, with particular regard to Personal Data;
- assess the sufficiency of the security measures, policies and procedures, information systems, technology and other arrangements that the Provider has in place to control such risks.

Risk Assessments must consider the implications of Data Protection Laws and any other applicable regulations, legal requirements and industry standards (including but not limited to SSAE 16 – SOC2, PCI—DSS and Cloud Security Alliance (CSA) where relevant and appropriate).

The Provider shall implement appropriate controls to manage the identified risks. Should the Client determine that the Provider has not remediated identified risks to a satisfactory level the Client reserves the right to commission and conduct its own risk assessment using a mutually agreed independent expert third party.

3. Access Control

The Provider shall ensure that appropriate Physical Access and Logical Access processes, procedures and security controls are in place to restrict access to any part of the Premises of the Provider where equipment or information related to the System or The Client Data is located or held to only those employees and contractors of the Provider and third parties engaged by the Provider, who are involved in delivering the Services and whose role requires them to have such access, provided on the principles of least privilege and segregation of duties.

3.1 Physical controls shall include but not be limited to:

- *Monitored electronic access control systems which uniquely identify individual access and maintain records of access for a minimum of 365 days;*
- *CCTV surveillance of access with recordings retained for a minimum of 30 days;*
- *Intrusion alarm systems with monitoring on a 24 x7 basis.*

The Provider shall ensure that the appropriate Logical Access procedures and security controls are in place to restrict access to any part of the System to employees and contractors of the Provider and third parties engaged by the Provider, who are involved in delivering of the Services and whose role requires them to have such access, provided on the principles of least privilege and segregation of duties.

The Provider shall ensure that all appropriate controls are implemented to restrict access to any part of the System and The Client Data by any user that remotely accesses the Provider's network.

3.2 Logical controls shall include but not be limited to:

- *Two factor authentication, notably for remote access*
- *Remote access device compliance validation (to verify at least Anti-Virus version and patch level)*

The Provider shall implement appropriate controls to ensure that:

- *Access to end user systems is automatically locked after a period of inactivity not exceeding 10 minutes after which re-authentication will be required;*
- *Passwords have a minimum length of not less than 8 characters;*
- *Password complexity requirements are enforced requiring at least three different types of character;*
- *Access is automatically disabled upon entry of no more than 5 incorrect passwords and access is not re-instated without verification of the identity of the user;*
- *Separate authentication credentials are provided to individuals requiring privileged access, e.g. system administrators, to be used solely for privileged access related activities'.*
- *All privileged access is logged with these logs kept secure, accurate and unmodified for at least 12 months.*
- *All privileged access rights are reviewed and recertified at least every 6 months.*
- *All access rights to sensitive or special categories of The Client Data are reviewed and recertified at least every 6 months.*
- *All other access rights (e.g. user accounts, service accounts) are reviewed and recertified at least every 12 months.*
- *Access to production systems will not be provided to those with a development role.*
- *Shared accounts are not permitted unless the activities of individual users of that account can be identified.*
- *Appropriate procedures are implemented to process access rights for Starters, Movers and Leavers that record the management of such access rights and can evidence the effectiveness of the above when requested by the Client.*
- *All assets and credentials (including but not limited to swipe cards, keys, userids, hardware/software tokens) used for the purposes of enabling access rights are retrieved, disabled and revoked on termination of the employment of an employee or contractor or similarly treated commensurate with any other change to the role and responsibilities of the employee or contractor accessing the Premises and The Client Data.*

The Provider shall ensure that all employees and contractors engaged in the provision of Services under the Agreement having Physical and/or Logical Access to Premises and/or The Client Data are under obligations of confidentiality no less stringent than the confidentially obligations imposed on the Provider under this Agreement.

4. Data Storage

The Provider shall ensure that all The Client Data which is electronically processed is encrypted or similarly protected when stored (regardless of storage media) in accordance with the Provider's Security Policy and Information Security Management System and ensuring compliance with Data Protection Laws and any other applicable regulations, legal requirements and industry standards. The Provider shall use an appropriate industry standard encryption method and industry standard key management practices and techniques.

4.1 Separation of data processing and storage

The Provider shall implement and maintain appropriate security measures and procedures to ensure that The Client Data collected for different purposes can be processed separately, including, but not limited to, the following:

- *Production systems shall not depend on development infrastructure;*
- *No production data shall be used for development testing without the explicit prior consent of Client which reserves the right to request additional controls in such cases;*
- *The development of new application or system software shall be kept separate from the production environment.*
- *The Client Data shall be logically and where possible physically separated from the data of other clients of the Provider and that of the Provider.*

5. Security in software development

The Provider shall ensure that software developed by the Provider which either forms part of the Services or could provide access to The Client Data is developed using secure coding practices such as OWASP or equivalent. Such software will undergo security testing during the development process to identify vulnerabilities. Any identified vulnerabilities shall be remediated prior to deployment.

6. Disposal/Destruction

The Provider shall ensure that any information held, whether original, reproduced or derived from The Client Data regardless of media shall be physically destroyed when no longer needed (e.g. due to technical redundancy) or can no longer be processed (e.g. through technical failure), and disposed of via an appropriate waste service.

The Provider shall ensure that any information held electronically, whether original, reproduced or derived from The Client Data regardless of media shall be made unreadable, where possible unintelligible, and unrecoverable, prior to media destruction and disposal.

Records of destruction must be retained and made available to The Client on request.

7. Data Transfer

The Provider shall ensure that electronic transfers of The Client Data over public / nonsecure network are undertaken securely using appropriate industry standard encryption methods and industry standard key management practices and techniques.

The Provider shall ensure that The Client Data is not stored on Portable Computing Devices or Portable Media unless appropriately encrypted. The Provider shall have appropriate technical controls to prevent unauthorised transfer of data to Portable Computing Devices and Portable Media.

8. Patch Management, Change Management and Technology Obsolescence Management

The Provider shall implement and maintain appropriate security measures and procedures in order to ensure the regular update and patching of all computer hardware, software and peripherals to eliminate vulnerabilities and remove flaws that could otherwise facilitate security breaches.

The Provider shall notify the Client of any significant change to the System (as set out in the respective provisions of the Agreement), including any Schedules relating to Change Control providing as much advanced notification as possible prior to the planned implementation of the Change Request.

The Provider shall notify the Client of any hardware, software or peripherals being used in the provision of services to The Client which will not be supported by the supplier(s) of such assets beyond the term of the relevant supplier agreement(s) and shall provide The Client with a documented plan to replace such assets at least 6 months before the end of support.

9. Vulnerability scanning and penetration testing

The Provider will undertake regular (at least monthly) vulnerability scanning of all systems which store or provide access to systems hosting The Client Data. This will include all Internet facing systems and APIs.

The Provider shall have penetration testing of all Internet facing applications and APIs used in connection with the provision of services to The Client on at least an annual basis and upon any material change. Such testing shall be undertaken by appropriately accredited entities and individuals.

Where Internet facing services use The Client branding, The Client reserves the right to conduct vulnerability scanning and or penetration testing of these services using an accredited independent expert third party and, where practical, will provide as much advanced notification of such activities as possible.

10. Intrusion Detection / Prevention and Malware

The Provider shall implement appropriate security measures and procedures to ensure that The Client Data, assets and / or systems being used to provide the Services are protected against the risk of intrusion and the effects of viruses, Trojan horses, worms, and other forms of attack. These measures include, but are not limited to, Intrusion Detection and Prevention Systems (IDS/IPS), firewalls (both internal and external), Network Access Control (NAC), Web Access Control (WAC) and Anti-malware.

The Provider shall implement appropriate monitoring systems, operational on a 24x7 basis, to detect intrusion to systems storing or having a means to access The Client Data.

11. Business Continuity, Backup and Recovery

The Provider shall comply with all Client's requirements (as set out in the respective provisions of the Agreement), including any Schedules relating to Business Continuity and / or Disaster Recovery. The Provider shall implement and maintain appropriate backup and recovery security measures and procedures in order to ensure data availability in the event of loss of data or information systems from any cause thereby ensuring that business continuity and disaster recovery plans align with the Client's requirements with particular reference to Recovery Point Objectives (RPO) and Recovery Time Objectives (RPO). Business continuity and disaster recovery plans shall be tested on a regular basis.

The Provider shall ensure that backups are encrypted using appropriate industry standard encryption methods and industry standard key management practices and techniques.

12. Incident Management / Reporting

The Provider shall put in place (and document for audit purposes) the necessary processes and procedures that will allow it to make all reasonable endeavours to detect any unauthorised Physical Access and Logical Access or other breaches of security.

The Provider shall establish and document, within 30 days of the commencement date, a 'Security Incident Response Procedure', which shall encompass the identification, qualification, quantification, classification and escalation of Security Incidents, their management and reporting and the process of confirmations of resolution.

The Provider shall notify The Client in writing immediately after becoming aware of any confirmed unauthorised access or other confirmed breach of security including Near Misses involving The Client Data, whether on the part of the Provider or a Subprocessor

13. Right of Audit

Subject to the relevant audit provisions included in the Agreement The Client's Information Security Management Team or their nominated auditors from time to time (including after any major Security Incident) may conduct a review of the security controls and procedures in place in relation to the Premises, the System, Physical Access and Logical Access as have been implemented for the purposes of providing the Services. This may include, but not necessarily limited to, an audit of:

- *Physical Access security controls;*
- *Logical Access security controls;*
- *Access Rights Management procedure documentation and records;*
- *Training provision documentation and records;*
- *Disposal/Destruction procedure documentation and records;*
- *Incident response procedure documentation and records;*
- *Use of remote access technologies;*
- *Monitoring and diagnostic tools;*
- *Management of security alerts and remedies;*
- *IT Change Requests; and*
- *Relevant Security Policies in place at the time (including Provider accreditations which whenever possible should be specific to the System and Services).*

The Client reserves the right to commission and conduct its own forensic investigation using a mutually agreed independent expert third party following a Security Incident.

The Provider shall provide on request responses to an Information Security Questionnaire for the purposes of measuring Information Security compliance. Client shall provide the questionnaire with at least 4 weeks' notice of the due date on an annual basis.

14. The Client Premises and Systems

When working at a Client (or Client Affiliate) premises or accessing Client (or Client Affiliate) systems, the Provider's employees and contractors shall comply with the relevant policies as advised by the relevant supervising manager.

15. Vetting/Recruitment

The Provider shall comply with all Client's requirements (as set out in the respective provisions of the Agreement), including any Schedules relating to screening and vetting of employees and contractors either prior to their employment/engagement or before any Physical Access and/or Logical Access is given to such individuals to The Client Data.

The Provider shall ensure that all employees and contractors having Physical and/or Logical Access to The Client Data are under obligations of confidentiality no less stringent than the confidentially obligations imposed on the Provider under the Agreement.

16. Sub-Contractors and Agents

Where the Provider has been authorised to engage sub-contractors and/or agents to provide some or all of the Services pursuant to the provisions of the Agreement, the Provider will impose contractual obligations on the respective subcontractors and/or agents (including without limitation suppliers, cleaning and maintenance staff) on terms substantially equivalent to those contained in this Schedule.

17. Service Levels

The Provider shall comply with all Client's requirements (as set out in the respective provisions of the Agreement), including any Schedules relating to Service Levels pertaining to the confidentiality, integrity and availability levels of the System and Services provided supported by the submission to the Client of periodic service control reports providing at minimum service level indicators and deviations, incidences of service, actions or changes in the service and relevant related risks.