d

MASTER SUBSCRIPTION AGREEMENT

Version 6.0

Subscription Agreement

DATE: ********** 202*

PARTIES:

(1) ***Invida Limited,*** a company incorporated in England and Wales (Registration number *10223226*) having its registered office at Celixir House, Stratford Business & Technology Park, Innovation Way, Stratford-upon-Avon, Warwickshire CV37 7GZ, United Kingdom (the "**Provider**"); and

(2) **********, a company incorporated in England and Wales (Registration number *********) having its registered office at ********** (the "**Customer**").

BACKGROUND:

(A) The Customer owns and operates certain facilities that require a software suite (the "**Platform**") to help manage and control activities. The Provider has developed a SAAS software solution, made available as a complete package or as distinct modules, to support these activities. The modules integrate with the INVIDA CORE module to extend functionality as and when needed with minimal cost and disruption.

(B) The Provider operates the Platform and provides the Support Services, and the Customer wishes to be granted access to the Platform and to receive the Support Services, on the terms of this Agreement.

AGREEMENT:

1. Definitions and interpretation

1.1 In this Agreement:

"2FA" means Two-factor Authentication identity and access management security method;

"**Affiliate**" means an entity that Controls, is Controlled by, or is under common Control with the relevant entity;

"**Agreement**" means this software as a service agreement (including the Schedules) and any amendments to it from time to time;

"**Business Day**" means any week day, other than a bank or public holiday in England;

"**Business Hours**" means between 09:00 and 17:00 London time on a Business Day;

"**Change**" means any change to the terms of this Agreement;

"**Charges**" means the amounts payable by the Customer to the Provider under or in relation to this Agreement (as set out in Schedule 3);

"**Confidential Information**" means the Customer Confidential Information and the Provider Confidential Information;

"Configuration" means the altering of settings and configuration options within the Platform as part of Set-up by the Provider to affect the functionality and look-and-feel of the Platform features;

"**Control**" means the legal power to control (directly or indirectly) the management of an entity (and "**Controlled**" will be construed accordingly);

"**Customer Confidential Information**" means:

(a) any information disclosed (whether disclosed in writing, orally or otherwise) by the Customer to the Provider that is marked as "confidential", described as "confidential" or should reasonably have been understood by the Provider at the time of disclosure to be confidential;

(b) the terms and conditions of this Agreement, and;

(c) the Customer Materials.

"**Customer Materials**" all data, works and materials:

(a) uploaded to, stored on, processed using or transmitted via the Platform by or on behalf of the Customer or by any person or application or automated system using the Customer's account, and;

(b) otherwise provided by the Customer to the Provider in connection with this Agreement;

"**Customer Portfolio**" means the Estate and or Properties owned or managed by the Customer (as amended from time to time) and identified as such in Schedule 1;

"**Customer Representatives**" means the person or persons (as amended from time to time) and identified as such in Schedule 1;

"**Customisations**" means customisations to the Platform that the Provider and Customer agree the Provider will produce on behalf of the Customer;

"Data Protection Legislation" means the Data Protection Act 2018 ("DPA"), the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), the General Data Protection Regulation ((EU) 2016/679) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR"), or similar legislation as implemented under English law (including any national implementing laws, regulations and secondary legislation), in each case as applicable and in force in the United Kingdom from time to time and all other Applicable Laws and regulations, relevant industry codes of practice and guidance issued by the Information Commissioner, supervisory authority or other bodies concerning the protection of personal data and privacy, as well as and where "**Controller**", "**data subject**", "**personal data**", "**personal data breach**", "**process**",

"**processor**" and "**supervisory authority**" are referred to in the Agreement they shall have the meanings set out in the Data Protection Legislation. References to Article numbers of the GDPR shall be deemed to include the equivalent provisions in the event the Article numbers in the legislation are changed from time to time;

"**Documentation**" means the documentation (including User Guides) produced by the Provider and supplied to the Customer specifying how the Platform should be used;

"**Effective Date**" means the date of execution of this Agreement;

"**Force Majeure Event**" means an event, or a series of related events, that is outside the reasonable control of the party affected (including failures of or problems with the internet or a part of the internet, hacker attacks, virus or other malicious software attacks or infections, power failures, industrial disputes affecting any third party, changes to the law, disasters, explosions, fires, floods, riots, terrorist attacks and wars);

"**Intellectual Property Rights**" means all intellectual property rights wherever in the world, whether registered or unregistered, including any application or right of application for such rights (and the "intellectual property rights" referred to above include copyright and related rights, database rights, confidential information, trade secrets, know-how, business names, trade names, trademarks, service marks, passing off rights, unfair competition rights, patents, petty patents, utility models, semi-conductor topography rights and rights in designs);

"**Minimum Term**" means the period specified as such in Schedule 1;

"**Modern Slavery Act**" means the Modern Slavery Act 2015;

"Modules" are discrete units of software applications, described as such, that are capable of functioning independently within the Platform and charged for as a discrete unit;

"**Permitted Purpose**" means the use of the Platform and its features to manage building assets and maintenance associated with assets directly owned / leased by the Customer and referred to in Schedule 1 as the Customer portfolio;

"**Personal Data**" has the meaning given to it in the Data Protection legislation;

"**Platform**" means the software platform known as INVIDA that is owned and operated by the Provider, made available to the Customer as a service via the internet under this Agreement, either as a complete package or limited to specific modules as detailed in Schedule 1;

"**Provider Confidential Information**" means:

(a) any information disclosed (whether disclosed in writing, orally or otherwise) by the Provider to the Customer that is marked as "confidential", described as "confidential" or should reasonably have been understood by the Customer at the time of disclosure to be confidential;

(b) the terms and conditions of this Agreement.

"**Provider Representatives**" means the person or persons (as amended from time to time) identified as such in Schedule 1;

"Representatives" means the Customer Representatives and the Provider Representatives;

"**Schedule**" means a schedule attached to this Agreement;

"**Services**" means all the services provided or to be provided by the Provider to the Customer under this Agreement, including the Support Services;

"Supervisory Authority" has the meaning given to it in Data Protection Legislation (and in any case, includes the UK Information Commissioner);

"**Support Services**" means support and maintenance services provided or to be provided by the Provider to the Customer in accordance with Schedule 2;

"Term" means the term of this Agreement;

"Upgrades" means new versions of, and updates to, the Platform, whether for the purpose of fixing an error, bug or other issue in the Platform or enhancing the functionality of the Platform; and

"**VAT**" means any value added tax or similar indirect sales taxes.

1.2 In this Agreement, a reference to a statute or statutory provision includes a reference to:

(a) that statute or statutory provision as modified, consolidated and/or re-enacted from time to time; and

(b) any subordinate legislation made under that statute or statutory provision.

1.3 The Clause headings do not affect the interpretation of this Agreement.

1.4 The ejusdem generis rule is not intended to be used in the interpretation of this Agreement.

1.5 A reference to a statute or statutory provision is a reference to it as it is in force for the time being, taking account of any amendment, extension, or re-enactment and includes any subordinate legislation for the time being in force made under it.

2. Term

This Agreement will come into force on the Effective Date and will continue in force for the Minimum Term and indefinitely thereafter, unless terminated in accordance with Clause 13.

3. The Platform

3.1 The Provider will make available the Platform to the Customer from the Effective Date.

3.2 Subject to the limitations set out in Clause 3.3 and the prohibitions set out in Clause 3.4, the Provider hereby grants to the Customer a non-exclusive licence to use the Platform for the Permitted Purpose via standard web browsers detailed in Schedule 1, and in accordance with the Documentation during the Term.

3.3 The licence granted by the Provider to the Customer under Clause 3.2 is subject to the following limitations:

(a) the Platform may only be used by the employees and agents of the Customer and:

(i) where the Customer is a company, the Customer's officers;

(ii) where the Customer is a partnership, the Customer's partners; and

(iii) where the Customer is a limited liability partnership, the Customer's members;

(b) the Platform may only be used in respect of the Customer Portfolio described in Schedule 1.

3.4 Except to the extent mandated by applicable law or expressly permitted in this Agreement, the licence granted by the Provider to the Customer under this Clause 3 is subject to the following prohibitions:

(a) the Customer must not sub-license its right to access and use the Platform or allow any unauthorised person to access or use the Platform;

(b) the Customer must not frame or otherwise re-publish or re-distribute the Platform;

(c) the Customer must not alter or adapt or edit the Platform save as expressly permitted by the Documentation; and

(d) the Customer may not share use of the Platform or the Platform features to allow the recording or management of the assets or buildings owned or managed by other organisations.

3.5 For the avoidance of doubt, the Customer has no right to access the object code or source code of the Platform, either during or after the Term.

3.6 All Intellectual Property Rights in the Platform shall, as between the parties, be the exclusive property of the Provider.

3.7 The Customer shall use reasonable endeavours to ensure that no unauthorised person will or could access the Platform using the Customer's account.

3.8 The Customer must not use the Platform in any way that causes, or may cause,

damage to the Platform or impairment of the availability or accessibility of the Platform, or any of the areas of, or services on, the Platform.

3.9 The Customer must not use the Platform:

(a) in any way that is unlawful, illegal, fraudulent or harmful; or

(b) in connection with any unlawful, illegal, fraudulent or harmful purpose or activity.

4. Support Services and Upgrades

4.1 During the Term the Provider will provide the Support Services to the Customer, and may apply Upgrades to the Platform, in accordance with the service level agreement set out in Schedule 2.

4.2 The Provider may sub-contract the provision of any of the Support Services without obtaining the consent of the Customer.

5. Customisations

5.1 From time to time the Provider and the Customer may agree that the Provider will customise the Platform in accordance with a specification agreed in writing between the parties.

5.2 From the date when a Customisation is first made available to the Customer, the Customisation shall form part of the Platform under the Agreement, and accordingly from that date the Customer's rights to use the Customisation shall be governed by Clause 3.

5.3 The Customer acknowledges that the Provider may make any Customisation available to its other Customers following the making available of that Customisation to the Customer.

5.4 All Intellectual Property Rights in the Customisations shall, as between the parties, be the exclusive property of the Provider.

6. Management

6.1 The Customer will ensure that instructions requesting modifications or configuration, and/or imports and exports of Customer Materials, in relation to this Agreement will be given by a Customer Representative to a Provider Representative, and the Provider:

(a) may treat all such instructions as the fully authorised instructions of the Customer; and

(b) will not comply with any other such instructions in relation to this Agreement without first obtaining the consent of a Customer Representative.

7. Customer Materials

7.1 The Customer grants to the Provider during the Term a non-exclusive licence to store, copy and otherwise use the Customer Materials on the Platform for the purposes of operating the Platform, providing the Services, fulfilling its other obligations under this Agreement, and exercising its rights under this Agreement.

7.2 Subject to Clause 7.1, all Intellectual Property Rights in the Customer Materials will remain, as between the parties, the property of the Customer.

7.3 The Customer warrants and represents to the Provider that the Customer Materials, and their use by the Provider in accordance with the terms of this Agreement, will not:

(a) breach any laws, statutes, regulations or legally-binding codes;

(b) infringe any person's Intellectual Property Rights or other legal rights; or

(c) give rise to any cause of action against the Provider or the Customer or any third party,

in each case in any jurisdiction and under any applicable law.

7.4 Where the Provider reasonably suspects that there has been a breach by the Customer of the provisions of this Clause 7, the Provider may:

(a) delete or amend the relevant Customer Materials; and/or

(b) suspend any or all of the Services and/or the Customer's access to the Platform while it investigates the matter.

7.5 Any breach by the Customer of this Clause 7 will be deemed to be a material breach of this Agreement for the purposes of Clause 13.

8. Charges

8.1 The Provider will issue via Email invoices in PDF format for the Charges to the Customer in accordance with the provisions of Schedule 3.

8.2 The Customer will pay the Charges to the Provider within 30 days of the date of issue of an invoice issued in accordance with Clause 8.1.

8.3 All Charges stated in or in relation to this Agreement are stated exclusive of VAT, unless the context requires otherwise. VAT will be payable by the Customer to the Provider in addition to the principal amounts.

8.4 Charges must be paid by bank transfer (using such payment details as are notified by the Provider to the Customer from time to time).

8.5 If the Customer does not pay any amount properly due to the Provider under or in connection with this Agreement, the Provider may:

(a) charge the Customer interest on the overdue amount at the rate of 2,5% per year above the base rate of Lloyds Bank Plc from time to time (which interest will accrue daily and be compounded quarterly); or

(b) claim interest and statutory compensation from the Customer pursuant to the Late Payment of Commercial Debts (Interest) Act 1998.

8.6 The Provider may vary the Charges payable under Paragraphs 2 and 3 of Schedule 3 on and from any anniversary of the Effective Date by giving to the Customer not less than 90 days' written notice of the variation, providing that:

(a) no such variation will result in the relevant element of the Charges increasing during the Term by more than the percentage increase during the same period in the Consumer Prices Index (all items) published by the UK Office for National Statistics, and

(b) no variation to the Charges payable under Paragraphs 2 and 3 of Schedule 3 will be made during the Minimum Term, charges remain fixed and not subject to increase during the Minimum Term.

8.7 The Provider may suspend access to the Platform and the provision of the Services if any undisputed amounts due to be paid by the Customer to the Provider under this Agreement are overdue by more than 30 days, subject to notice of such failure to pay any undisputed amounts. The Provider shall afford the Customer ten (10) Business Days to remedy any non-payment prior to exercising such right of suspension.

9. Warranties

9.1 The Provider warrants and represents that it conducts its business in a manner that is consistent with the Modern Slavery Act 2015.

9.2 The Customer warrants and represents to the Provider that it has the legal right and authority to enter into and perform its obligations under this Agreement.

9.3 The Provider warrants and represents to the Customer:

(a) that it has the legal right and authority to enter into and perform its obligations under this Agreement; that it will perform its obligations under this Agreement with reasonable care skill and diligence to be expected of a properly qualified and competent provider experienced in the provisions of such services;

(b) that the Platform will perform substantially in accordance with the Documentation (subject to any Upgrades and Customisations);

(c) that the Platform will be hosted in accordance with the requirements set out in Schedule 1, and will be available to the Customer in accordance with the uptime commitments given in Schedule 2;

(d) the Platform (excluding for the avoidance of doubt the Customer Materials) will not infringe any person's Intellectual Property Rights in any jurisdiction and under any applicable law; and

(e) the Platform is and will remain free from viruses and other malicious software programs.

9.4 The Customer acknowledges that:

(a) complex software is never wholly free from defects, errors and bugs, and the Provider gives no warranty or representation that the Platform will be wholly free from such defects, errors and bugs;

(b) the Provider does not warrant or represent that the Platform will be compatible with any application, program or software not specifically identified as compatible in Schedule 1; and

(c) the Provider will not and does not purport to provide any legal, taxation or accountancy advice under this Agreement or in relation to the Platform and the Provider does not warrant or represent that the Platform will not give rise to any civil or criminal legal liability on the part of the Customer or any other person.

9.5 All of the parties' warranties and representations in respect of the subject matter of this Agreement are expressly set out in the terms of this Agreement. To the maximum extent permitted by applicable law, no other warranties or representations concerning the subject matter of this Agreement will be implied into this Agreement.

10. Limitations and exclusions of liability

10.1 Nothing in the Agreement will:

(a) limit or exclude the liability of a party for death or personal injury resulting from its negligence or the negligence of its personnel, agents or subcontractors;

(b) limit or exclude the liability of a party for fraud or fraudulent misrepresentation by that party;

(c) limit any liability of a party in any way that is not permitted under applicable law; or

(d) exclude any liability of a party that may not be excluded under applicable law.

10.2 The limitations and exclusions of liability set out in this Clause 10:

(a) are subject to Clause 10.1; and

(b) govern all liabilities arising under the Agreement or in relation to the subject matter of the Agreement, including liabilities arising in contract, in tort (including negligence) and for breach of statutory duty.

10.3 Neither party to this Agreement shall have any liability to the other party, whether in contract, tort (including negligence), breach of statutory duty or otherwise, for any indirect or consequential loss arising under or in connection with this Agreement.

10.4 Neither party will be liable for any losses arising out of a Force Majeure Event.

10.5 The Provider's liability in relation to any event or series of related events will not exceed the total amount paid and payable by the Customer to the Provider under the Agreement during the 12-month period immediately preceding the event or events giving rise to the claim.

11. Data protection

11.1 With respect to the parties' rights and obligations under this Contract, the parties agree that the Customer is the Data Controller and that the Provider is the Data Processor. “Controller”, “Processor”, “Data Subject” and “Personal Data” shall have the meaning as set out in the Data Protection Act 2018. “Process” shall also have the meaning given to it under the Data Protection Legislation but, for the purposes of this Contract, it shall include both manual and automatic processing.

11.2 The Customer warrants that it has the legal right to disclose all Personal Data that it does in fact disclose to the Provider under or in connection with this Agreement.

11.3 The parties have set out in Schedule 5 - Data Processing Annexure the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects (which may be updated from time to time).

11.4 The Provider warrants that in relation to any Personal Data it shall:

a) Process the Personal Data only in accordance with written instructions from the Customer or his representative (which may be specific instructions or instructions of a general nature as set out in this Contract or as otherwise notified by the Customer or his representative to the Provider during the Term);

b) Process the Personal Data only to the extent, and in such manner, as is necessary for the provision of the Services or as is required by Law or any Regulatory Body;

c) Implement appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected;

d) Take reasonable steps to ensure the reliability of any staff who have access to the Personal Data;

e) Obtain prior written consent from the Customer or his representative in order to transfer the Personal Data to any sub-contractors or affiliates for the provision of the service;

f) Ensure that all Provider*'s* staff required to access the Personal Data are informed of the confidential nature of the Personal Data and comply with the obligations set out in this clause; and

g) Ensure that none of Provider*'s* personnel publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Customer or his representative.

11.5 The Provider shall notify the Customer or his representative (within five Business Days) if it receives:

a) a request from a Data Subject to have access to that person's Personal Data; or

b) a complaint or request relating to the Customer's obligations under the Data Protection Legislation;

11.6 The Provider shall notify the Customer or his representative of any data breach in respect of the Personal Data without unreasonable delay.

11.7 The Provider shall fully cooperate and assist the Customer or his representative in relation to any complaint or request made, including by:

(a) providing the Customer or his representative with full details of the complaint or request;

(b) complying with a data access request within the relevant timescales set out in the Data Protection Legislation and in accordance with the Customer or his representative's instructions;

(c) providing the Customer or his representative with any Personal Data it holds in relation to a Data Subject (within the timescales required by the Customer or his representative); and

(d) providing the Customer or his representative with any information requested by the Customer or his representative.

11.8 The Provider shall permit the Customer or his representative (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit the Provider's Data Processing activities (and/or those of its agents, subsidiaries and sub-contractors) and comply with all reasonable requests or directions by the Customer or his representative to enable the Customer or his representative to verify and/or procure that the Provider is in full compliance with its obligations under this Contract.

11.9 The Provider shall provide a written description of the technical and organisational methods employed by the Provider for processing Personal Data (within the timescales required by the Customer or his representative).

11.10 The Provider shall not process personal Data outside the European Economic Area without the prior written consent of the Customer or his representative and, where the Customer or his representative consents to a transfer, to comply with any reasonable instructions notified to it by the Customer or his representative.

11.11 The Provider shall comply at all times with the Data Protection Legislation and shall not perform its obligations under this Contract in such a way as to cause the Customer or his representative to breach any of its applicable obligations under the Data Protection Legislation.

11.12 Each party agrees that in the performance of its respective obligations under the Agreement it shall comply with all applicable statues, laws, secondary legislation, rules, regulations and guidance from any relevant supervisory authority relating to privacy, confidentiality, security, direct marketing or data protection of personal data or corporate data (including any national laws implementing any such legislation) including the Data Protection Legislation.

12. Confidentiality and publicity

12.1 The Provider will:

(a) keep confidential and not disclose the Customer Confidential Information to any person save as expressly permitted by this Clause 12;

(b) protect the Customer Confidential Information against unauthorised disclosure by using the same degree of care as it takes to preserve and safeguard its own confidential information of a similar nature, being at least a reasonable degree of care;

(c) without prejudice to the generality of Clause 12.1(b), deploy and maintain the security systems and technologies detailed in Schedule 1 in relation to the Customer Confidential Information held on the Platform;

(d) unless the customer specifically denies such consent, be permitted to use the Customer's data to facilitate industry benchmarking, provided that such data is anonymous and aggregated to a sufficient degree, meaning that data could not be specifically associated with any individual client of The Provider.

12.2 The Customer will:

(a) keep confidential and not disclose the Provider Confidential Information to any person save as expressly permitted by this Clause 12;

(b) protect the Provider Confidential Information against unauthorised disclosure by using the same degree of care as it takes to preserve and safeguard its own confidential information of a similar nature, being at least a reasonable degree of care.

12.3 Confidential Information of a party may be disclosed by the other party to that other party's officers, employees, agents, insurers and professional advisers, provided that the recipient is bound in writing to maintain the confidentiality of the

Confidential Information disclosed.

12.4 The obligations set out in this Clause 12 shall not apply to:

(a) Confidential Information that is publicly known (other than through a breach of an obligation of confidence);

(b) Customer Confidential Information that is received by the Provider, and Provider Confidential Information that is received by the Customer, from an independent third party who has a right to disclose the relevant Confidential Information; or

(c) Confidential Information that is required to be disclosed by law, or by a governmental authority, stock exchange or regulatory body, provided that the party subject to such disclosure requirement must where permitted by law give to the other party prompt written notice of the disclosure requirement.

12.5 Neither party will make any public disclosure relating to this Agreement (including press releases, public announcements and marketing materials) without the prior written consent of the other party.

13. Termination

13.1 Either party may terminate this Agreement immediately by giving written notice to the other party if the other party:

(a) commits any material breach of any term of this Agreement, and:

(i) the breach is not remediable; or

(ii) the breach is remediable, but the other party fails to remedy the breach within 30 days of receipt of a written notice requiring it to do so; or

(b) persistently breaches the terms of this Agreement (irrespective of whether such breaches collectively constitute a material breach).

13.2 Either party may terminate this Agreement immediately by giving written notice to the other party if:

(a) the other party:

(i) is dissolved;

(ii) ceases to conduct all (or substantially all) of its business;

(iii) is or becomes unable to pay its debts as they fall due;

(iv) is or becomes insolvent or is declared insolvent; or

(v) convenes a meeting or makes or proposes to make any arrangement

or composition with its creditors;

(b) an administrator, administrative receiver, liquidator, receiver, trustee, manager or similar is appointed over any of the assets of the other party;

(c) an order is made for the winding up of the other party, or the other party passes a resolution for its winding up (other than for the purpose of a solvent company reorganisation where the resulting entity will assume all the obligations of the other party under this Agreement); or

(d) (where that other party is an individual) that other party dies, or as a result of illness or incapacity becomes incapable of managing his or her own affairs, or is the subject of a bankruptcy petition or order.

13.3 Either party may terminate this Agreement by giving at least 90 days' written notice of termination to the other party, subject to the expiration of the Minimum Term set out in Schedule 1.

13.4 The Provider may terminate the Agreement immediately by giving written notice of termination to the Customer where the Customer fails to pay to the Provider any undisputed amount due to be paid under the Agreement within 90 days of the due date.

14. Effects of termination

14.1 Upon termination of this Agreement, all the provisions of this Agreement will cease to have effect, save that the following provisions of this Agreement will survive and continue to have effect (in accordance with their terms or otherwise indefinitely): Clauses 3.5, 3.6, 12, and 18.6.

14.2 Termination of this Agreement will not affect either party's accrued liabilities and rights as at the date of termination.

14.3 Subject to Clause 14.5, within 30 days following the termination of the Agreement, the Provider will:

(a) irrevocably delete from the Platform all Customer Confidential Information; and

(b) irrevocably delete from its other computer systems all Customer Confidential Information, and return to the Customer or dispose of as the Customer may instruct all documents and materials containing Customer Confidential Information.

(c) return to the Customer a digital copy of all Customer Materials stored within the Platform on solid-state portable storage devices with records presented in Microsoft Excel or CSV files and all document attachments presented in folder structures containing files in their original form (doc, pdf, jpg etc.).

14.4 Subject to Clause 14.5, within 30 days following the termination of this Agreement, the Customer will:

(a) return to the Provider or dispose of as the Provider may instruct all documents and materials containing Provider Confidential Information; and

(b) irrevocably delete from its computer systems all Provider Confidential Information.

14.5 A party may retain any document (including any electronic document) containing the Confidential Information of the other party after the termination of this Agreement if:

(a) that party is obliged to retain such document by any law or regulation or other rule enforceable against that party; or

(b) the document in question is a letter, fax, email, order confirmation, invoice, receipt or similar document addressed to the party retaining the document.

15. Anti-Slavery and Human Trafficking

15.1 In performing its obligations under this Agreement, the Provider shall, and shall ensure that all Providers Personnel shall, comply with the Modern Slavery Act.

15.2 The Provider represents and warrants that neither it nor any of its Providers Personnel other persons associated with it:

(a) has been convicted of any offence involving slavery and human trafficking; and

(b) to the best of its knowledge, has been or is the subject of any investigation, inquiry or enforcement proceedings by any governmental, administrative or regulatory body regarding any offence or alleged offence of or in connection with slavery and human trafficking.

15.3 The Provider shall implement due diligence procedures for all Providers Personnel in its supply chains, to ensure that there is no slavery or human trafficking in such supply chains.

15.4 The Provider shall notify the Customer as soon as it becomes aware of:

(a) any breach, or potential breach, of the Modern Slavery Act;

(b) any actual or suspected slavery or human trafficking in a supply chain which has a connection with this Agreement; or

(c) any act or omission by the Provider or the Providers Personnel that will, or is reasonably likely to, put the Customer in breach of its obligations under the Modern Slavery Act.

15.5 At the Customer's request, the Provider shall prepare and deliver to the Customer, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply

chains or in any part of its business.

15.6 The Provider shall maintain a complete set of records to trace the supply chain of all Services provided to the Customer in connection with this Agreement.

15.7 The Provider shall implement a system of training for the Providers Personnel to ensure compliance with the Modern Slavery Act.

15.8 The Provider shall keep a record of all training offered and completed by all Provider Personnel to ensure compliance with the Modern Slavery Act and shall make a copy of the record available to the Customer on request.

15.9 The Provider represents, warrants and undertakes that it conducts its business in a manner that is consistent with the Modern Slavery Act.

15.10 Breach of this Clause 15 shall be deemed an irremediable material breach under Clause 13.1(a).

16. Notices

16.1 Any notice given under this Agreement must be in writing (whether or not described as "written notice" in this Agreement) and must be delivered personally, sent by recorded signed-for post, or sent by email, for the attention of the relevant person, and to the relevant address or email address given below (or as notified by one party to the other in accordance with this Clause).

The Provider:

Invida Limited, Celixir House, Stratford Business & Technology Park, Innovation Way, Stratford-upon-Avon, Warwickshire CV37 7GZ, United Kingdom, commercial@invida.co.uk

The Customer:

**********, **********, ****, ****

16.2 A notice will be deemed to have been received at the relevant time set out below (or where such time is not within Business Hours, when Business Hours next begin after the relevant time set out below):

(a) where the notice is delivered personally, at the time of delivery;

(b) where the notice is sent by recorded signed-for post, 48 hours after posting; and

(c) where the notice is sent by email, at the time of the transmission (providing the sending party retains written evidence of the transmission).

17. Force Majeure Event

17.1 Where a Force Majeure Event gives rise to a failure or delay in either party performing its obligations under this Agreement (other than obligations to make payment), those obligations will be suspended for the duration of the Force Majeure Event.

17.2 A party who becomes aware of a Force Majeure Event which gives rise to, or which is likely to give rise to, any failure or delay in performing its obligations under this Agreement, will:

(a) forthwith notify the other; and

(b) will inform the other of the period for which it is estimated that such failure or delay will continue.

17.3 The affected party will take reasonable steps to mitigate the effects of the Force Majeure Event.

18. General

18.1 No breach of any provision of this Agreement will be waived except with the express written consent of the party not in breach.

18.2 If a Clause of this Agreement is determined by any court or other competent authority to be unlawful and/or unenforceable, the other Clauses of this Agreement will continue in effect. If any unlawful and/or unenforceable Clause would be lawful or enforceable if part of it were deleted, that part will be deemed to be deleted, and the rest of the Clause will continue in effect (unless that would contradict the clear intention of the parties, in which case the entirety of the relevant Clause will be deemed to be deleted).

18.3 Nothing in this Agreement will constitute a partnership, agency relationship or contract of employment between the parties.

18.4 This Agreement may not be varied except in accordance with a written document signed by or on behalf of each of the parties.

18.5 Each party hereby agrees that the other party may assign (only with prior written consent) any or all of its contractual rights and/or obligations under this Agreement to any Affiliate of the assigning party or any successor to all or a substantial part of the business of the assigning party from time to time. Save as expressly provided in this Clause or elsewhere in this Agreement, neither party may without the prior written consent of the other party assign, transfer, charge, license or otherwise dispose of or deal in this Agreement or any contractual rights or obligations under this Agreement.

18.6 Neither party will, without the other party's prior written consent, either during the term of this Agreement or within 6 months after the date of effective termination of this Agreement, engage, employ or otherwise solicit for employment any employee, agent or contractor of the other party who has been involved in the performance of this Agreement.

18.7 Each party agrees to execute (and arrange for the execution of) any documents and do (and arrange for the doing of) any things reasonably within that party's power, which are necessary to enable the parties to exercise their rights and fulfil their obligations under this Agreement.

18.8 This Agreement is made for the benefit of the parties, and is not intended to benefit any third party or be enforceable by any third party. The rights of the parties to terminate, rescind, or agree any amendment, waiver, variation or settlement under or relating to this Agreement are not subject to the consent of any third party.

18.9 Subject to Clause 10.1:

(a) this Agreement and the end user licence agreement referred to in herein constitutes the entire agreement between the parties in relation to the subject matter of this Agreement, and supersedes all previous agreements, arrangements and understandings between the parties in respect of that subject matter; and

(b) neither party will have any remedy in respect of any misrepresentation (whether written or oral) made to it upon which it relied in entering into this Agreement.

18.10 This Agreement will be governed by and construed in accordance with the laws of England and Wales; and the courts of England will have exclusive jurisdiction to adjudicate any dispute arising under or in connection with this Agreement.

19. Counterparts

This Agreement may be executed in any number of counterparts, and by each party on separate counterparts, but shall not be effective until both parties have each executed at least one counterpart. Each counterpart shall constitute an original of this Agreement, but all the counterparts shall together constitute but one and the same instrument.

The parties have indicated their acceptance of this Agreement by executing it below.

EXECUTION:

SIGNED by

duly authorised for and on behalf
of the Provider

.....

Date:

SIGNED by

duly authorised for and on behalf
of the Customer

.....

Date:

Schedule 1- Miscellaneous

Minimum Term

The Minimum Term shall be the period of 36 months following the Effective Date.

Modules

Under the terms of this agreement the Provider will make available to the Customer the INVIDA platform with the following Modules included:

- CORE (including Portfolio and Surveys)
- ***
- ***
- ***
- ***

Customer Portfolio

The estate, comprising of ******* with an estimated size of and estimated **m2 as set out in the Providers Proposal dated ******

The Platform supports the following web browsers:

- Microsoft Edge
- Chrome (recommended)
- Safari

Concurrent Users:

- Unlimited

Customer Representatives:

****
E: *@****.uk
T: *****
M: *****

Provider Representatives:

****
E: ***.****@invida.co.uk
T: 0333 335 0041
M:*********

Schedule 2 – Service Level Agreement

1. Introduction

1.1 In this Schedule:

"**New Functionality**" means new functionality that is introduced to the Platform by an Upgrade; and

1.2 References in this Schedule to Paragraphs are to the paragraphs of this Schedule, unless otherwise stated.

2. Service Desk

2.1 The Provider will make available, during Business Hours, a telephone and email service desk facility for the purposes of:

(a) assisting the Customer with the configuration of the Platform and the integration of the Platform with the Customer's other systems;

(b) assisting the Customer with the proper use of the Platform; and/or

(c) determining the causes of errors and fixing errors in the Platform.

(d) Service Desk No: 0333 335 004 – Email: support@invida.co.uk - available 09:00 to 17:00 GMT. Emergencies outside of these hours will be managed via mobile telephone by the Nominated Account Manager. Contact details are included in “Provider Representatives” in this agreement

2.2 Subject to Paragraph 2.3, the Customer must make all requests for Support Services through the service desk, and all such requests must include at least the following information: Customer name; User name; description of the problem and/or assistance required; indication of the priority of the case.

2.3 The Provider will use reasonable endeavours to ensure that a member of its support staff can be reached by mobile phone outside Business Hours in the case of an emergency.

3. Response and resolution times

3.1 The Provider will:

(a) use reasonable endeavours to respond to requests for Support Services made through the service desk; and

(b) use reasonable endeavours to resolve issues raised by the Customer, in accordance with the following response time matrix.

Severity	Examples	Maximum Response time	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)
Critical	Platform not available; significant reduction in performance	30 minutes	30 minutes	24 hours
Serious	Loss or corruption of Customer Materials, loss of specific features or functionality	30 minutes	1 hour	24 hours
Moderate	Resetting of passwords, data integrity issues	30 minutes	4 hours	N/A
Minor	Application support, guidance on features and usage of the Platform, general instruction	30 minutes	8 hours	N/A

3.2 The Provider will determine, acting reasonably, in to which severity category an issue raised through the Support Services falls.

3.3 All Support Services will be provided remotely unless expressly agreed otherwise by the Provider.

4. Limits on Support Services

4.1 The Provider shall have no obligation under this Agreement to provide Support Services in respect of any fault or error caused by:

(a) the improper use of the Platform; or

(b) the use of the Platform otherwise than in accordance with the Documentation.

5. Upgrades

5.1 The Customer acknowledges that from time to time during the Term the Provider may apply Upgrades to the Platform, and that such Upgrades may, result in changes the appearance and/or functionality of the Platform.

5.2 The Provider will give to the Customer at least 30 days' prior written notice of the application of any significant Upgrade to the Platform. Such notice shall include details of the specific changes to the functionality of the Platform resulting from the application of the Upgrade.

6. Uptime commitment

6.1 The Provider shall use all reasonable endeavours to ensure that the Platform is available 99.95% of the time during each calendar month, subject to Paragraph 8.

6.2 In the event that, during a calendar month entirely within the Term, the Platform fails to meet the availability commitment set out in Paragraph 6.1 then the Provider shall issue service credits calculated in accordance with Paragraph 6.3 to the Customer, such service credits to be deducted by the Provider from future Charges.

6.3 Subject to Paragraph 6.4, the services credits referred to in Paragraph 6.2 and due in respect of a calendar month shall be calculated as follows:

service credits = ((100 - a) / 10) x b

where:

a = the actual percentage availability of the Platform during the relevant calendar month; and

b = the Charges payable in respect of access to the Platform during the relevant calendar month (exclusive of VAT and other taxes).

6.4 The maximum service credits available to the Customer in respect of any calendar month shall be the total Charges payable in respect of access to the Platform during the relevant calendar month (exclusive of VAT and other taxes).

6.5 Subject to Clause 11.1, then the award of service credits under this Paragraph 6 shall be the exclusive remedy of the Customer in the case of a failure of the provider to meet the uptime commitment in Paragraph 6.1 except in the case of a failure constituting a material breach of this Agreement.

6.6 In the event that Platform is not available or suffers a significant reduction in performance, the Provider will use all reasonable endeavours to achieve a target Recovery Time Objective (RTO) of within 30 minutes.

7. Back-up and restoration

7.1 Subject to Paragraph 7.2, the Provider will:

(a) make back-ups of the Customer Materials stored on the Platform on a daily basis, and will retain such back-ups for at least 14 days; and

(b) at least once every day, the Provider will arrange for the off-site storage of a current back-up of the Customer Materials stored on the Platform (which will be over-written on the following off-site back-up date).

7.2 In the event of the loss of, or corruption of, Customer Materials stored on the Platform being notified by the Customer to the Provider under Paragraph 2, the Provider shall if so directed by the Customer use all reasonable endeavours promptly to restore the Customer Materials from the most recent available back-up copy, with the aim of achieving a Recovery Point Objective (RPO) of within 24 hours.

8. Scheduled maintenance

8.1 The Provider may suspend access to the Platform in order to carry out scheduled maintenance, such maintenance to be carried out outside Business Hours and such suspension to be for not more than 8 hours in each calendar month.

8.2 The Provider must give to the Customer at least 14 days' written notice of schedule maintenance, including full details of the expected Platform downtime.

8.3 Platform downtime during scheduled maintenance carried out by the Provider in accordance with this Paragraph 8 shall not be counted as downtime for the purposes of Paragraph 6.

Schedule 3 - Charges

1. Introduction

1.1 References in this Schedule to Paragraphs are to the paragraphs of this Schedule, unless otherwise stated.

1.2 The Charges under the Agreement will consist of the following elements:

(a) set up Charges, in respect to deployment/s of the Platform;

(b) access Charges, in respect of access to and use of the Platform; and

(c) other Support Services Charges.

2. Set up Charges

2.1 Charges in the amount of £**,*** plus VAT in respect of the deployment of the Platform, including configuration, which shall be invoiced upon signature of this agreement.

2.2 Should the Customer wish to add additional modules to the subscription agreement then the additional Set-up charges will become due immediately. There is no obligation on the part of the Customer to subscribe to additional modules.

3. Access Charges

3.1 The Access Charge in the amount of £*,***, will be a fixed amount plus VAT per calendar month, which shall be invoiced by the Provider quarterly in advance at any time following the commencement of the calendar month in respect of which the Access Charges are incurred (such amount to be pro-rated by the Provider in the event that this Agreement came into force or was terminated during a calendar month).

3.2 Should the Customer wish to add additional modules to the subscription agreement, then the access charges will become due in accordance with clause 3.1 above. There is no obligation on the part of the Customer to subscribe to additional modules.

4. True-up/down adjustment

4.1 The Access Charges will be varied in the event that;

(a) the actual floor area of the portfolio is greater than, or less than, the estimated floor area used to determine the Access charges set out in Clause 3 (using the same basis of measurement set out in Schedule 1) and this results in the portfolio size moving into a different Charging Band, up or down, by reference to the Standard Schedule of Charges set out in Clause 4.3 and 4.4 below, the Access charges will be adjusted to reflect that increase or decrease.

(b) the floor area of the portfolio as determined under (a) above, increases by, or decreases by greater than 20%, and results in the portfolio size moving into a different Pricing Band, up or down, by reference to the Standard Schedule of

Charges set out in Clause 4.3 and 4.4 below, the Access charges will be adjusted to reflect that increase or decrease.

(c) any Access Charge changes contemplated under (a) and (b) shall apply from the point that that the calculation is made and agreed between the parties and shall not be backdated.

4.2 The True-up/down calculation will be performed on a bi-annual (twice per year) basis within 2 weeks of the six month and yearly anniversary, from of the date of signature of this agreement.

4.3 Standard schedule of charges – Charging Bands

Band	*Portfolio size (total GIA of multiple properties*	
	from	*to*
A	0 m^2	50,000 m^2
B	50,000 m^2	150,000 m^2
C	150,000 m^2	300,000 m^2
D	300,000 m^2	700,000 m^2
E	700,000 m^2	1,500,000 m^2
F	1,500,000 m^2	4,000,000 m^2
G	4,000,000 m^2	10,000,000 m^2
H	10,000,000 m^2	30,000,000 m^2

4.4 Standard schedule of charges – Monthly Access Charge (invoiced quarterly in advance)

	Charging Band							
Module	A	B	C	D	E	F	G	H
CORE	£990	£1,320	£1,980	£2,640	£3,300	£4,290	£5,280	£5,940
LIFECYCLE	£660	£924	£1,320	£1,980	£2,640	£3,300	£3,960	£4,620
COMPLIANCE	£396	£660	£924	£1,320	£1,980	£2,640	£3,300	£3,960
TASK	£1,650	£2,640	£3,960	£5,940	£7,920	£9,900	£11,550	£13,860
LIBRARY	£396	£660	£924	£1,320	£1,980	£2,640	£3,300	£3,960
PROJECT	£908	£1,546	£2,392	£3,550	£4,680	£5,980	£7,010	£8,160

5. Other Support Services Charges

5.1 In addition to the Charges detailed in Paragraphs 2 and 3 above, the Provider will invoice in respect of, and the Customer shall pay to the Provider Charges relating to any additional Support Services procured by the Customer.

5.2 Support Services Charges are to be calculated by reference to an hourly or daily rate as set out in the schedule below.

Support Services	*Rate*	*Basis*
Training (sessions of up to 10 users on client's premises)	£800	Per day
Training – Online (using Teams, Zoom, or WebEx)	£120	Per hour
Project Management / IT Consultancy	£1,200	Per day
Data Integration and configuration	£990	Per day
Data cleanse and bulk import	£800	Per day
Digitising and binding of CAD floorplans	£530	Per day
Implementation/testing of API integration with remote applications	£990	Per day
Travel expenses to and from client sites	£ at cost	

Schedule 4 – Data security and disaster recovery

1. Introduction

1.1 The Provider shall use all reasonable endeavours to ensure that the following systems and processes identified in this Schedule 4 remain in place during the Term to ensure the protection and availability of the Platform and Customer Materials stored on the Platform.

2. Cloud features and datacentres

2.1 The Platform is a public cloud model hosted on secure servers by Amazon AWS providing high-levels of reliability, scalability, performance and security. The Provider will continue to use this service during the Term, or provide written notification to the Customer if it intends to transfer the provision of such services to an alternative, and comparable provider.

2.2 The Customer will have access to its own installation of the Invida product, hosted on a secure AWS server. The Provider will monitor the performance of the application and may from time-to-time upgrade the server, or transfer the Customer's instance to a different server in order to improve the performance of the application if required. Such upgrades will take place in periods where the application is not in use, or at a time agreed with the Customer.

2.3 The Platform is hosted within TIA-942 Tier 3 datacentres located in cities within the UK and adhere to the EU code for energy efficient datacentres.

2.4 The Platform is managed by staff directly employed by the Provider based in the UK. Employment checks our carried out on all staff, and physical access control systems are in place at the Provider's offices.

2.5 Any access by the Provider to the servers or databases that store customer data is carried out over a secure VPN (Virtual Private Network) connection, which is secured by MFA (multi factor authentication).

3. Data storage, back-up and deletion

3.1 Customer Materials are stored in segregated SQL Server 2019 databases, allowing for data to be easily exported in a standard format as required.

3.2 The Provider shall store all of the Customers Data on persistent storage media in order to retain data in the event of a power outage.

3.3 The provider will perform nightly incremental backups which will be stored within the Amazon S3 cloud. All backups will be replicated to a separate availability zone within the EU.

3.4 Data-in-transit protection between user device and the Platform is provided through TLS encryption (HTTPS or VPN technologies).

3.5 Data-at-rest protection is provided through a combination of authentication and encryption.

4. Platform security, vulnerability management and testing

4.1 The Platform uses the industry standard OAuth 2.0 framework to ensure user authentication and authorisation to access the services.

4.2 The Provider will make available the option to enforce the use of 2FA (two factor authentication) by use of a TOTP (Time-based One Time Password) code system for additional security when authenticating users.

4.3 The Provider will monitor potential threats, vulnerabilities or exploitation techniques which could affect the Platform, and take corrective actions.

4.2 The Provider will schedule periodic independent vulnerability scan testing on a weekly basis, and penetration tests to be carried out on at least an annual basis or when significant updates are released.

4.3 All Platform events are recorded and routinely monitored and analysed for suspicious activity.

4.4 All file attachments uploaded to and downloaded from the Invida platform are systematically scanned using malware scanning tools.

5. Disaster recovery procedures

5.1 The Provider will maintain a disaster recovery (DR) process and procedures to mitigate the risks associated with a geographical disaster, loss of hosting services, and malicious acts such as cyber-attacks using malware and viruses.

5.2 Through the procedures set out within the disaster recovery processes, the Provider will use reasonable endeavours to ensure minimal loss of Platform availability, data integrity and availability. Such processes include:

a) clearly defined roles and responsibilities for those leading and delivering the DR procedures;

b) out-of-hours contact details for all staff and service providers required to invoke the DR procedures;

c) emergency contact details for Customer Representatives;

d) DR incident management flow diagrams;

e) data classification;

f) critical equipment details;

g) DR infrastructure diagram;

h) disaster assessment for potential threats, including: probability rating; impact rating; and, remedial actions;

i) Incident management process.

Schedule 5 – Data Processing Annexure

1. Processing Personal Data

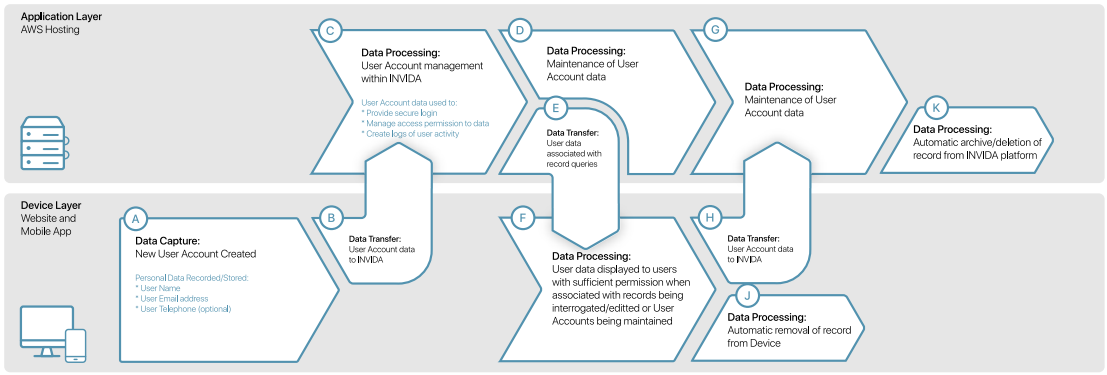
1.1 Customer Materials uploaded to the Provider's Platform exclude Personal Data, except for Personal Data held by the Provider to enable controlled access by authorised Customer employees and agents to the Platform, as set out below.

Description	Details
Duration of the Processing	From the effective date of this Master Subscription Agreement through to termination of this agreement in accordance with Clause 14 Termination and Clause 15 Effects of termination.
Nature and purposes of the Processing	The personal data set out in Clause 6.1 above will be recorded, processed and transferred in the management of user accounts to ensure secure login to the Platform and to maintain web server access logs in order to analyse site traffic, debug problems, and defend against security attacks.
Type of Personal Data	*a)* User Name *b)* Email Address *c)* Contact telephone number (optional)
Categories of Data Subject	Customer Representatives, Customer employees and agents of the Customer.
Plan for return and destruction of the data once the Processing is complete	Upon termination the Provider will erase all Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy in accordance with Clause 15.3 (a).

2. Data processing instructions

1.1 Process and data flow will be as set out below in Fig. 2.1

Fig. 2.1



1.2 The INVIDA Mobile App will typically be used by the Customer to carry out asset surveys. Personal data will be transferred between the App and the INVIDA servers via a standard JSON RESTful Web Service.

a) The App requests only the data that is relevant to the jobs assigned to the user who is currently logged in, and therefore the data transferred is limited only to that scope. Whilst in transit, the data is encrypted via HTTPS, and once the data is received by the App, it is decrypted and stored locally within a database on the device.

b) The information about the job is retained on the device until the job is completed, plus a configurable number of days to allow the user to access historic information. The current default for this configuration is 7 days. Once this retention period has expired, the information will be wiped from the device the next time it performs a data synchronisation, which currently happens at regular intervals (the exact interval is controlled by the device itself, but it normally every hour, or when the App is opened by the user). Furthermore, when the user "logs out" from the app, all data is purged from the local database.

2.3 When a user accesses the INVIDA web portal, all data is accessed via a secure JSON RESTful Web Service. The website requests only the data relevant to the specific action being carried out by the user. Depending on the activity being undertaken, this can sometimes include the Names, Email Addresses and Phone Numbers of people who have been set up as Users, or who have been registered as key contacts within the application.

a) Whilst in transit, the data is encrypted via HTTPS, and once received it is only stored within memory on the computer or device accessing the service, it does not get routinely saved to disk, cached or stored.

a) The data is retained in memory until the user navigates away from the page in question, at which point it is marked for deletion. The actual deletion from memory is controlled by the web browser itself. The data will also be deleted from memory if the web browser is closed, or the user navigates away.

Schedule 6 – Cyber Security

1. Cyber and Data Insurance

1.1 The Provider shall at its own expense obtain and maintain: (i) cyber and data insurance with a minimum per claim limit of indemnity of not less than £250,000 for each claim (including costs), to cover the Provider's potential liabilities under or in connection with Clause 2; and (ii) in force such cover, during the term of this Agreement and for a period of at least 3 years following its expiry or termination. The Provider shall, on request by the Customer from time to time, provide the Customer with evidence of such cover and payment of related insurance premiums.

2. Cyber Security

2.1 For the purposes of this Clause 2:

"Customer Data" means all data, information, text and drawings owned by or otherwise licensed or provided to any member of the Customer Group, and all Customer Personal Data, which are embodied in any electronic or tangible medium and are provided to the Provider or otherwise accessed, used or held by the Provider in the provision of the Services including all relevant data compiled or created in connection with the arrangements set out in this Agreement whether acquired by the Provider or provided by or on behalf of the Customer during the course of this Agreement;

"Customer Personal Data" means any and all personal data (as defined in EU Directive 95/46/EC or its replacement from time to time (Data Protection Law)) in respect of which the Customer is a controller or processor, in each case as defined in the Data Protection Law;

"Good Industry Practice" means using the standard of skill, care, knowledge and foresight which would reasonably and ordinarily be expected from an experienced person engaged in providing services which are the same as, or similar to, the Services;

"Removable Media" means portable or removable hard disks, including laptops, tablets or smartphone hard disks, floppy disks, Universal Serial Bus (USB) memory drives, zip disks, optical disks, CDs, DVDs, digital film, memory cards (Secure Digital , Memory Sticks, Compact Flash, SmartMedia, MultiMediaCard and xD-Picture Cards, magnetic tape, and all other removable media storage;

"Security Breach" means any security breach relating to any Customer Data (or the systems on which such data reside), including, without limitation, any loss or theft of, or unauthorised access to, the Customer Data; and

"Security Feature" means any security feature including, without limitation, any key, PIN or password.

2.2 The Provider shall ensure that the Customer Data is kept secure and confidential. The Provider shall use all appropriate technical and organisational security measures, practices and systems, and all appropriate and up-to-date Security Features, to prevent, and take prompt and proper remedial action against, unauthorised access, copying, modification, storage, reproduction, display or distribution of the Customer Data and any accidental loss of or damage to the Customer Data and to preserve the integrity of

the Customer Data.

2.3 The Provider shall ensure that all Customer Data is kept in encrypted form in accordance with Good Industry Practice.

2.4 The Provider shall use best industry standard anti-virus software and the latest virus definitions to protect the Customer Data against viruses.

2.5 The Provider shall ensure that all Security Features are kept confidential and not lent, shared, transferred or otherwise misused by the Provider or any third party.

2.6 The Provider shall screen all individuals that may come into contact with the Customer Data or otherwise provide the Services, for potential security risks and require all such individuals to sign appropriate confidentiality/non-disclosure agreements. All agreements with third parties involving access to the Provider's systems and data, including all outsourcing arrangements and maintenance and support agreements (including facilities maintenance), shall specifically address security risks, cyber risks, controls and procedures for information systems. The Provider shall supply each of its personnel and contractors with appropriate, on-going training regarding information and cyber security procedures, risks and threats. The Provider shall have an established set of procedures to ensure that all employees and contractors promptly report actual and/or suspected breaches of security. The Provider shall procure that each of its sub-contractors complies with the provisions of this Clause 2.

2.7 The Provider shall:

(a) Document and provide the Customer with copies of all relevant security policies and standards (including escalation procedures for non-compliance) for the Customer's review;

(b) complete any security questionnaire the Customer may submit to the Provider from time to time; and

(c) comply with the Client's security policies notified to the Supplier from time to time.

2.8 The Provider will schedule periodic independent penetration tests to be carried out on at least an annual basis or when significant updates are released, and agree to share the findings of these tests with the Customer in order to monitor the effectiveness of the Provider's security measures taken in connection with the protection of Customer Data. In addition, and upon request, the Provider shall promptly permit the performance of additional vulnerability threat assessment tests, penetration tests and / or such testing as may be reasonably and periodically required by the Customer, at the Customer's expense.

2.9 The Provider shall make a back-up copy of the Customer Data in accordance with Good Industry Practice and record the copy on media from which the Customer Data can be reloaded in the event of any corruption or loss of the Customer Data. Each such back-up shall form part of the Customer Data.

2.11 If the Provider:

(a) becomes aware of any actual or potential unauthorised or unlawful processing of any Customer Data or that any Customer Data has been lost or destroyed or has become damaged, corrupted or unusable, or of any other actual or potential attacks or security incidents affecting the Customer Data or the systems on which the Customer Data reside;

(b) becomes aware of any actual or potential Security Breach; or

(c) learns or suspects that any Security Feature has been revealed to or obtained by any unauthorised person,

the Provider shall, at its own expense: (i) immediately notify the Customer (and follow-up in writing); (ii) fully co-operate with the Customer to remedy the issue as soon as reasonably practicable; (iii) conduct or support the Customer in conducting computer forensic investigations and any other analysis that the Customer reasonably requires; and (iv) implement any actions or remedial measures which the Customer considers necessary as a result of the breach including, without limitation, carrying out credit monitoring services for any individuals affected by any of the events referred to in this Clause 2.11 in accordance with Good Industry Practice.

2.12 The Provider shall: (i) return all Customer Data to the Customer on request; and (ii) at the Customer's option, promptly following the date this Agreement terminates, either return such data to the Customer or destroy it in accordance with the Customer's reasonable security requirements (and provide the Customer with written confirmation of such secure destruction).