

This Aerona Online Services Agreement ("the Agreement") is a legal agreement between you ("the Customer") and Aerona Software Services Limited with registered office at 2nd Floor, Embassy Building, 3 Strand Road, Derry City, Co. Derry, Northern Ireland, BT48 7BH and registered number NI47827 ("the Supplier") for the purposes of Practice Management Software that is instantly accessible and easy to use, and delivered as an application hosted over the web.

IF YOU PURCHASE OUR SERVICES, THIS AGREEMENT WILL ALSO GOVERN YOUR PURCHASE AND ONGOING USE OF THOSE SERVICES.

(1) BY ACCEPTING THIS AGREEMENT, EITHER BY WRITING BY AGREEING ORDER FORM OR BY PROCEEDING WITH THE USE OF AERONADENTAL OR AERONACLINIC, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY AND ITS AFFILIATES TO THESE TERMS AND CONDITIONS, IN WHICH CASE THE TERM "THE CUSTOMER" SHALL REFER TO SUCH ENTITY AND ITS AFFILIATES. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT USE THE SOFTWARE OR HOSTING SERVICES, MAINTENANCE AND SUPPORT.

BACKGROUND

- (A) The Supplier has developed certain software applications and platforms which it makes available to subscribers via the internet on a pay-per-use basis for the purpose of Practice Management, including data processing.
- (B) The Customer wishes to use the Supplier's service in its business operations.
- (C) The Supplier has agreed to provide and the Customer has agreed to take and pay for the Supplier's service subject to the terms and conditions of this agreement.

AGREED TERMS

1. INTERPRETATION

- 1.1 The definitions and rules of interpretation in this clause apply in this agreement.

Authorised Users: those employees, agents and independent contractors of the Customer who are authorised by the Customer to use the Services, as described in the Order Form and updated pursuant to clause 2.2(d).

Back Up Policy: as described in Schedule 1.

Business Day: any day which is not a Saturday, Sunday or public holiday in the UK.

1

Business Purpose: the processing of Data strictly in order to provide the Services.

Commencement Date: unless otherwise agreed and set out in the Order Form, the date that you start using the Services.

Confidential Information: information that is proprietary or confidential and is either clearly labelled as such or identified as Confidential Information in clause 11.5.

Customer Data: the data inputted by the Customer, Authorised Users, or the Supplier on the Customer's behalf for the purpose of the Services.

Data: any data or information, in whatever form, including Personal Data, Sensitive Personal Data, images, still and moving, and sound recordings, the processing of which comprises the Services (wholly or in part).

Data Controller: has the meaning set out in the PDPR.

Data Processor: has the meaning set out in the PDPR.

Data Subject: has the meaning set out in the PDPR.

Data Processing Policy: the arrangements in place between the Supplier and the Customer in relation to processing by the Supplier of Personal Data and Sensitive Personal Data outlined in Schedule Five.

Employee Access Policy: the Supplier's policy for employee access set out in Schedule 3.

Minimum Term: the initial term of this agreement as set out in the Order Form.

Normal Business Hours: 9 am to 5 pm local UK time, each Business Day.

Order Form: the document agreed by the Customer and Supplier which sets out a description of the Services, the Commencement Date, the Minimum Term and the number of User Subscriptions in the form appended hereto at Schedule 2.

Personal Data: has the meaning set out in the PDPR.

Privacy and Data Protection Requirements (PDPR): the Data Protection Act 1998, the General Data Protection Regulations (*Regulation (EU) 2016/79*), the Data Protection Directive (95/46/EC), 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 (*SI 2426/2003*) and all applicable laws and regulations relating to the processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information

Commissioner or any other supervisory authority, and the equivalent of any of the foregoing in any relevant jurisdiction.



Processed Data: any Customer Data that has been processed.

Relevant Data: the Customer Data and the Processed Data.

Renewal Period: the period described in clause 14.1.

Security Breach: any security breach relating to the Customer Data reasonably determined by the Supplier to be sufficiently serious or substantial to justify notification to the Information Commissioner or other relevant supervisory authority in accordance with the PDPR.

Security & Privacy Policy: the Supplier's policy on data security and privacy set out in Schedule 4.

Sensitive Personal Data: has the meaning set out in the PDPR.

Services: the subscription services provided by the Supplier to the Customer under this agreement via a website notified to the Customer by the Supplier from time to time, as more particularly described in the Order Form, and including (inter alia) user instructions, service descriptions and API documentation and the processing of Data.

Software: the online software applications provided by the Supplier as part of the Services.

Subscription Fees: the subscription fees payable by the Customer to the Supplier for the User Subscriptions, as agreed in the Order Form, or as subsequently amended pursuant to clauses 3, 9.5 or 9.6.

Subscription Term: has the meaning given in clause 14.1.

Supplier System: any information technology system or systems owned or operated by the Supplier to which Data is delivered or on which the Services are performed in accordance with this agreement.

Technical and Organisational Security Measures: those measures aimed at protecting Personal Data and Sensitive Personal Data against accidental or unlawful destruction or accidental or unauthorised loss, alteration, unauthorised disclosure or access, in particular here the processing involves the transmission of data over a network, and against all other unlawful forms of processing including as described in the Data Processing Policy, the Security and Privacy Policy and the Back Up Policy.

User Subscriptions: the user subscriptions purchased by the Customer which entitle Authorised Users to access and use the Services as set out in the Order Form in accordance with this agreement.

Virus: any thing or device (including any software, code, file or programme) which may: prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any

telecommunications service, equipment or network or any other service or device; prevent, impair or otherwise adversely affect access to or the operation of any programme or data, including the reliability of any programme or data (whether by re-arranging, altering or erasing the programme or data in whole or part or otherwise); or adversely affect the user experience, including worms, trojan horses, viruses and other similar things or devices.

1.2 Clause, schedule and paragraph headings shall not affect the interpretation of this agreement.

1.3 A person includes an individual, corporate or unincorporated body (whether or not having separate legal personality) and that person's legal and personal representatives, successors or permitted assigns.

1.4 A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established.

1.5 Words in the singular shall include the plural and vice versa.

1.6 A reference to one gender shall include a reference to the other genders.

1.7 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.

1.8 References to clauses and schedules are to the clauses and schedules of this agreement; references to paragraphs are to paragraphs of the relevant schedule to this agreement.

2. USER SUBSCRIPTIONS

2.1 Subject to the Customer purchasing the User Subscriptions in accordance with clause 3.3 and clause 9.1, the restrictions set out in this clause 2 and the other terms and conditions of this agreement, the Supplier hereby agrees to provide the Services to, and make them available for use by, the Customer and its Authorised Users on a non-exclusive, non-transferable basis during the Subscription Term solely for the Customer's internal business operations.

2.2 In relation to the Authorised Users, the Customer undertakes that:

- (a) the maximum number of Authorised Users that it authorises to access and use the Services shall not exceed the number of User Subscriptions it has purchased from time to time;
- (b) it will not allow or suffer any User Subscription to be used by more than one individual Authorised User unless it has been reassigned in its entirety to another individual Authorised User, in which case the prior Authorised User shall no longer have any right to access or use the Services;
- (c) each Authorised User shall keep a secure password for his use of the Services, that such password shall be changed no less frequently than monthly and that each Authorised User shall keep his password confidential;
- (d) it shall maintain a written, up to date list of current Authorised Users and provide such list to the Supplier within 5 Business Days of the Supplier's written request at any time or times;
- (e) it shall permit the Supplier to audit the Services in order to establish the name and password of each Authorised User. Such audit may be conducted no more than once per quarter, at the Supplier's expense, and this right shall be exercised with reasonable prior notice, in such a manner as not to substantially interfere with the Customer's normal conduct of business;
- (f) if any of the audits referred to in clause 2.2(e) reveal that any password has been provided to any individual who is not an Authorised User, then without prejudice to the Supplier's other rights, the Customer shall promptly disable such passwords and the Supplier shall not issue any new passwords to any such individual; and
- (g) if any of the audits referred to in clause 2.2(e) reveal that the Customer has underpaid Subscription Fees to the Supplier, the Customer shall pay to the Supplier an amount equal to such underpayment as calculated in accordance with the prices agreed at inception with the individual Customer within 10 Business Days of the date of the relevant audit.

2.3 The Customer shall not access, store, distribute or transmit any Viruses, or any material during the course of its use of the Services that:

- (a) is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;
- (b) facilitates illegal activity;
- (c) depicts sexually explicit images;
- (d) promotes unlawful violence;

- (e) is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability, or any other illegal activity; or
- (f) causes damage or injury to any person or property;

and the Supplier reserves the right, without liability to the Customer, to disable the Customer's access to any material that breaches the provisions of this clause.

2.4 The Customer shall not:

- (a) except as may be allowed by any applicable law (including where appropriate the United Kingdom and Ireland) which is incapable of exclusion by agreement between the parties:
 - (i) and except to the extent expressly permitted under this agreement, attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Software in any form or media or by any means; or
 - (ii) attempt to reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Software; or
- (b) access all or any part of the Services in order to build a product or service which competes with the Services; or
- (c) use the Services to provide services to third parties; or
- (d) subject to clause 19.1, license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Services available to any third party except the Authorised Users, or
- (e) attempt to obtain, or assist third parties in obtaining, access to the Services, other than as provided under this clause 2.

2.5 The Customer shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the Services and, in the event of any such unauthorised access or use, promptly notify the Supplier.

2.6 The rights provided under this clause 2 are granted to the Customer only, and shall not be considered granted to any subsidiary or holding company of the Customer.

3. ADDITIONAL USER SUBSCRIPTIONS

3.1 Subject to clause 3.2 and clause 3.3, the Customer may, from time to time during any Subscription Term, purchase additional User Subscriptions in excess of the number agreed at inception with the individual Customer and the Supplier shall grant access to the Services to such additional Authorised Users in accordance with the provisions of this agreement.

3.2 If the Customer wishes to purchase additional User Subscriptions, the Customer shall notify the Supplier in writing. The Supplier shall evaluate such request for additional User Subscriptions and respond to the Customer with approval or disapproval of the request, such approval not to be unreasonably withheld.

3.3 If the Supplier approves the Customer's request to purchase additional User Subscriptions, the Customer shall, on the date of the Supplier's invoice, pay to the Supplier the relevant fees for such additional User Subscriptions as agreed with the individual Customer and, if such additional User Subscriptions are purchased by the Customer part way through the Minimum Term or any Renewal Period (as applicable), such fees shall be pro-rated for the remainder of the Minimum Term or then current Renewal Period (as applicable).

4. SERVICES

4.1 The Supplier shall, during the Subscription Term, provide the Services to the Customer on and subject to the terms of this agreement.

4.2 The Supplier shall use commercially reasonable endeavours to make the Services available 24 hours a day, seven days a week, except for:

- (a) planned maintenance carried out during the maintenance window of 9 pm to 12:00 am UK time; and
- (b) unscheduled maintenance performed outside Normal Business Hours, provided that the Supplier has used reasonable endeavours to give the Customer at least 6 Normal Business Hours' notice in advance.

4.3 The Supplier will, as part of the Services and at no additional cost to the Customer, provide the Customer with the Supplier's standard customer support services during Normal Business Hours. This will cover e-mail and telephone support. The Customer may purchase enhanced support services separately at the Supplier's then current rates.

- 4.4 The Supplier shall not act on any specific instructions given by the Customer from time to time during the Term unless they are:
- (a) in writing; and
 - (b) given by an Authorised Person (**Specific Instructions**).
- 4.5 The Supplier shall process the Customer Data for the Business Purpose only and in compliance with the Customer's instructions from time to time and in accordance with the Data Processing Policy.
- 4.6 The Customer acknowledges that the Supplier is under no duty to investigate the completeness, accuracy or sufficiency of any Specific Instructions or the Customer Data.

5. DATA PROCESSING

- 5.1 The Customer shall own all rights, title and interest in and to all of the Customer Data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of the Customer Data.
- 5.2 The Supplier shall in providing the Services adhere to its Security & Privacy Policy, Employee Access Policy, Back Up Policy and the Data Processing Policy.
- 5.3 In the event of any loss or damage to Customer Data, the Customer's sole and exclusive remedy shall be for the Supplier to use reasonable commercial endeavours to restore the lost or damaged Customer Data from the latest back-up of such Customer Data maintained by the Supplier in accordance with the archiving procedure described in its Back-Up Policy. The Supplier shall not be responsible for any loss, destruction, alteration or disclosure of Customer Data caused by any third party (except those third parties sub-contracted by the Supplier to perform services related to Customer Data maintenance and back-up).
- 5.4 The Supplier's obligations under clause 5.3 shall be performed at the Customer's reasonable expense, except to the extent that the Security Breach arose out of any negligence or wilful default of the Supplier or any breach by the Supplier of its warranties in clause 12.

6. THIRD PARTY PROVIDERS

The Customer acknowledges that the Services may enable or assist it to access the website content of, correspond with, and purchase products and services from, third parties via third-party websites and that it does so solely at its own risk. The Supplier makes no representation or commitment and shall have no liability or obligation whatsoever in relation to the content or use of, or correspondence with, any such third-party website, or any transactions completed, and any contract entered into by the Customer, with any such third party. Any contract entered into and any transaction completed via any third-party website is between the Customer and the relevant third party, and not the Supplier. The Supplier recommends that the Customer refers to the third party's website terms and conditions and privacy policy prior to using the relevant third-party website. The Supplier does not endorse or approve any third-party website nor the content of any of the third-party website made available via the Services.

7. SUPPLIER'S OBLIGATIONS

7.1 The Supplier undertakes that the Services will be performed substantially in accordance with the Order Form and with reasonable skill and care and in compliance with the Data Processing Policy.

7.2 The Supplier shall:

- (a) only make copies of the Customer Data to the extent reasonably necessary for the Business Purpose (which, for clarity, includes back-up, mirroring (and similar availability enhancement techniques), security, disaster recovery and testing of the Customer Data);
- (b) not extract, re-utilise, use, exploit, redistribute, re-disseminate, copy or store the Customer Data other than for the Business Purpose; and
- (c) not do anything that may materially damage the reputation of the Customer.

7.3 The Supplier shall ensure the reliability of all its employees who have access to the Customer Data and ensure that they comply with the provisions set out in the Data Processing Policy and in the Employee Access Policy.

7.4 The undertaking at clause 7.1 shall not apply to the extent of any non-conformance which is caused by use of the Services contrary to the

Supplier's instructions, or modification or alteration of the Services by any party other than the Supplier or the Supplier's duly authorised contractors or agents. If the Services do not conform with the foregoing undertaking, Supplier will, at its expense, use all reasonable commercial endeavours to correct any such non-conformance promptly, or provide the Customer with an alternative means of accomplishing the desired performance. Such correction or substitution constitutes the Customer's sole and exclusive remedy for any breach of the undertaking set out in clause 7.1.

Notwithstanding the foregoing, the Supplier:

- (a) does not warrant that the Customer's use of the Services will be uninterrupted or error-free; nor that the Services and/or the information obtained by the Customer through the Services will meet the Customer's requirements; and
- (b) is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Customer acknowledges that the Services may be subject to limitations, delays and other problems inherent in the use of such communications facilities.

7.5 This agreement shall not prevent the Supplier from entering into similar agreements with third parties, or from independently developing, using, selling or licensing documentation, products and/or services which are similar to those provided under this agreement.

7.6 The Supplier warrants that it has and will maintain all necessary licences, consents, and permissions necessary for the performance of its obligations under this agreement.

8. CUSTOMER'S OBLIGATIONS

The Customer shall:

- (a) provide the Supplier with:
 - (i) all necessary co-operation in relation to this agreement; and
 - (ii) all necessary access to such information as may be required by the Supplier;

in order to render the Services, including but not limited to Customer Data, security access information and configuration services;

- (b) comply with all applicable laws and regulations with respect to its activities under this agreement (including where applicable those of Ireland);
- (c) carry out all other Customer responsibilities set out in this agreement in a timely and efficient manner. In the event of any delays in the Customer's provision of such assistance as agreed by the parties, the Supplier may adjust any agreed timetable or delivery schedule as reasonably necessary;
- (d) ensure that the Authorised Users use the Services in accordance with the terms and conditions of this agreement and shall be responsible for any Authorised User's breach of this agreement;
- (e) obtain and shall maintain all necessary licences, consents, and permissions necessary for the Supplier, its contractors and agents to perform their obligations under this agreement, including without limitation the Services;
- (f) ensure that its network and systems comply with the relevant specifications provided by the Supplier from time to time; and
- (g) be solely responsible for procuring and maintaining its network connections and telecommunications links from its systems to the Supplier's data centres, and all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to the Customer's network connections or telecommunications links or caused by the internet.

9. CHARGES AND PAYMENT

9.1 The Customer shall pay the Subscription Fees to the Supplier for the User Subscriptions in accordance with this clause 9.

9.2 The Customer shall on the Commencement Date provide to the Supplier valid, up- to-date and complete payment method details and the Customer shall pay each invoice within 30 days after the date of such invoice.

9.3 If the Supplier has not received payment within 30 days after the due date, and without prejudice to any other rights and remedies of the Supplier:

- (a) the Supplier may, without liability to the Customer, disable the Customer's password, account and access to all or part of the Services and the Supplier shall be under no obligation to provide any or all of the Services while the invoice(s) concerned remain unpaid; and
- (b) interest shall accrue on such due amounts at an annual rate equal to 3% over the then current base lending rate of the Supplier's bankers in the UK at the date the relevant invoice was issued,

commencing on the due date and continuing until fully paid, whether before or after judgment.

- 9.4 All amounts and fees stated or referred to in this agreement:
- (a) shall be payable as stated in UK pounds sterling (GBP) or euros (EUR);
 - (b) are non-cancellable and non-refundable;
 - (c) are exclusive of value added tax or goods and services taxes. UK value added tax will be charged to UK business Customers at the appropriate rate as designated by HM Revenue & Customs. Where a non-UK EU business Customer is registered for Value Added Tax in their own jurisdiction they will provide the Supplier with their value added tax number and will self-account for value added tax on the supply. Where a non-UK EU business Customer is not registered for value added tax, then the business Customer is responsible for value added tax in their own jurisdiction. No value added tax will apply to supplies to non-EU Customers. The need for non-EU goods and services tax to apply to non-EU Customers will be reviewed on a contract by contract basis.
- 9.5 If, at any time whilst using the Services, the Customer exceeds the amount of data storage space agreed between the parties, the Supplier shall charge the Customer, and the Customer shall pay, the Supplier's then current excess data storage fees.
- 9.6 The Supplier shall be entitled to increase the Subscription Fees, the fees payable in respect of the additional User Subscriptions purchased pursuant to clause 3.3 and/or the excess storage fees payable pursuant to clause 9.5 at the start of each Renewal Period upon 90 days' prior notice to the Customer.

10. PROPRIETARY RIGHTS

- 10.1 The Customer acknowledges and agrees that the Supplier and/or its licensors own all intellectual property rights in the Services. Except as expressly stated herein, this agreement does not grant the Customer any rights to, or in, patents, copyrights, database rights, trade secrets, trade names, trademarks (whether registered or unregistered), or any other rights or licences in respect of the Services.
- 10.2 The Supplier confirms that it has all the rights in relation to the Services that are necessary to grant all the rights it purports to grant under, and in accordance with, the terms of this agreement.

11. CONFIDENTIALITY

11.1 Each party may be given access to Confidential Information from the other party in order to perform its obligations under this agreement. A party's Confidential Information shall not be deemed to include information that:

- (a) is or becomes publicly known other than through any act or omission of the receiving party;
- (b) was in the other party's lawful possession before the disclosure;
- (c) is lawfully disclosed to the receiving party by a third party without restriction on disclosure;
- (d) is independently developed by the receiving party, which independent development can be shown by written evidence; or
- (e) is required to be disclosed by law, by any court of competent jurisdiction or by any regulatory or administrative body (including where applicable those of Ireland).

11.2 The Supplier acknowledges that the Customer's Confidential Information includes any Customer Data.

11.3 Each party shall hold the other's Confidential Information in confidence and, unless required by law (including without limitation that of the United Kingdom and Ireland), not make the other's Confidential Information available to any third party, or use the other's Confidential Information for any purpose other than the implementation of this agreement.

11.4 Each party shall take all reasonable steps to ensure that the other's Confidential Information to which it has access is not disclosed or distributed by its employees or agents in violation of the terms of this agreement.

11.5 Neither party shall be responsible for any loss, destruction, alteration or disclosure of Confidential Information caused by any third party.

11.6 The Customer acknowledges that details of the Services, and the results of any performance tests of the Services, constitute the Supplier's Confidential Information.

11.7 This clause 11 shall survive termination of this agreement, however arising.

12. WARRANTIES

12.1 The Supplier warrants that it will process the Customer Data in compliance with the PDPR and the Data Processing Policy.

12.2 The Supplier warrants and represents that it will:

- (a) having regard to the cost of implementing the Technical and Organisational Security Measures and to technological development, Processor shall implement the security measures set out in Schedule Four and measures to ensure a level of security appropriate to the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage to personal data and/or sensitive personal data, and to reflect the nature of the personal data and/or sensitive personal data to be protected. The Supplier shall notify the Customer of any actual or anticipated breaches of its security (including where the personal data and/or sensitive personal data have been put at risk of any unauthorised or accidental access) which are likely to or actually affect the personal data and/or sensitive personal data or its security immediately, and at least within 24 hours of, becoming aware of such breaches.
- (b) take all reasonable steps to ensure compliance with those measures; and
- (c) discharge its obligations under this agreement, and under the Data Processing Policy, with all due skill, care and diligence.

12.3 The Customer warrants and represents that:

- (a) it is not aware of any circumstances likely to give rise to breach of any of the PDPR in the future (including any Security Breach);
- (b) the Supplier is entitled to process the Customer Data for the Business Purpose and such use will comply with all PDPR;
- (c) all Customer Data is necessary, accurate and up-to-date; and
- (d) it is registered with all relevant data protection authorities to process all Customer Data for the Business Purpose.

12.4 The Supplier does not warrant that the Processed Data:

- (a) is or are accurate, complete, reliable, secure, useful, fit for purpose or timely;
- (b) has or have been tested for use by the Customer or any third party; or
- (c) will be suitable for or be capable of being used by the Customer or any third party.

13. INDEMNITY

13.1 The Customer shall defend, indemnify and hold harmless the Supplier against claims, actions, proceedings, losses, damages, expenses and costs (including without limitation court costs and reasonable legal fees) arising out of or in connection with the Customer's use of the Services, provided that:

- (a) the Customer is given prompt notice of any such claim;
- (b) the Supplier provides reasonable co-operation to the Customer in the defence and settlement of such claim, at the Customer's expense; and
- (c) the Customer is given sole authority to defend or settle the claim.

13.2 The Supplier shall, subject to clause 13.3, defend the Customer, its officers, directors and employees against any claim that the Services infringes any United Kingdom or EU patent effective as of the Effective Date, copyright, trade mark, database right or right of confidentiality, and shall indemnify the Customer for any amounts awarded against the Customer in judgment or settlement of such claims, provided that:

- (a) the Supplier is given prompt notice of any such claim;
- (b) the Customer provides reasonable co-operation to the Supplier in the defence and settlement of such claim, at the Supplier's expense; and
- (c) the Supplier is given sole authority to defend or settle the claim.

13.3 In the defence or settlement of any claim, the Supplier may procure the right for the Customer to continue using the Services, replace or modify the Services so that they become non-infringing or, if such remedies are not reasonably available, terminate this agreement on 2 Business Days' notice to the Customer without any additional liability or obligation to pay liquidated damages or other additional costs to the Customer.

13.4 In no event shall the Supplier, its employees, agents and sub-contractors be liable to the Customer to the extent that the alleged infringement is based on:

- (a) a modification of the Services by anyone other than the Supplier; or
- (b) the Customer's use of the Services in a manner contrary to the instructions given to the Customer by the Supplier; or

- (c) the Customer's use of the Services after notice of the alleged or actual infringement from the Supplier or any appropriate authority.

13.5 The foregoing states the Customer's sole and exclusive rights and remedies, and the Supplier's (including the Supplier's employees', agents' and sub-contractors') entire obligations and liability, for infringement of any patent, copyright, trade mark, database right or right of confidentiality.

14. LIMITATION OF LIABILITY

14.1 Subject to the provisions of clause 12 this clause 13 sets out the entire financial liability of the Supplier (including any liability for the acts or omissions of its employees, agents and sub-contractors) to the Customer in respect of:

- (a) any breach of this agreement;
- (b) any use made by the Customer of the Services and or any part of them; and
- (c) any representation, statement or tortious act or omission (including negligence) arising under or in connection with this agreement.

14.2 Except as expressly and specifically provided in this agreement:

- (a) the Customer assumes sole responsibility for results obtained from the use of the Services by the Customer, and for conclusions drawn from such use. The Supplier shall have no liability for any damage caused by errors or omissions in any information, instructions or scripts provided to the Supplier by the Customer in connection with the Services, or any actions taken by the Supplier at the Customer's direction;
- (b) all warranties, representations, conditions and all other terms of any kind whatsoever implied by statute or common law are, to the fullest extent permitted by applicable law, excluded from this agreement; and
- (c) the Services are provided to the Customer on an "as is" basis.

14.3 The Supplier shall not in any circumstances be liable whether in contract, tort (including for negligence and breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, for:

- (a) any loss (whether direct or indirect) of profits, business, business opportunities, revenue, turnover, reputation or goodwill;
- (b) any loss or corruption (whether direct or indirect) of Data or information (other than as is provided in the PDPR);

- (c) loss (whether direct or indirect) of anticipated savings or wasted expenditure (including management time); or
- (d) any loss or liability (whether direct or indirect) under or in relation to any other contract.

14.4 Nothing in this agreement excludes the liability of the Supplier:

- (a) for death or personal injury caused by the Supplier's negligence; or
- (b) for fraud or fraudulent misrepresentation.

14.5 Subject to clause 13.2 and clause 13.3:

- (a) the Supplier shall not be liable whether in tort (including for negligence or breach of statutory duty), contract, misrepresentation, restitution or otherwise for any loss of profits, loss of business, depletion of goodwill and/or similar losses or loss or corruption of data or information, or pure economic loss, or for any special, indirect or consequential loss, costs, damages, charges or expenses however arising under this agreement; and
- (b) the Supplier's total aggregate liability in contract, tort (including negligence or breach of statutory duty), misrepresentation, restitution or otherwise, arising in connection with the performance or contemplated performance of this agreement shall be limited to the total Subscription Fees paid for the User Subscriptions during the 12 months immediately preceding the date on which the claim arose.

15. TERM AND TERMINATION

15.1 This agreement shall, unless otherwise terminated as provided in this clause 14, commence on the Effective Date and shall continue for the Minimum Term and, thereafter, this agreement shall be automatically renewed for successive periods of 1 month or 1 year as specified by the customer (each a **Renewal Period**), unless:

- (a) either party notifies the other party of termination, in writing, before the end of the Minimum Term or any Renewal Period, in which case this agreement shall terminate upon the expiry of the applicable Minimum Term or Renewal Period; or
- (b) otherwise terminated in accordance with the provisions of this agreement;

and the Minimum Term together with any subsequent Renewal Periods shall constitute the **Subscription Term**.

15.2 Without prejudice to any other rights or remedies to which the parties may be entitled, either party may terminate this agreement without liability to the other if:

- (a) the other party commits a material breach of any of the terms of this agreement and (if such a breach is remediable) fails to remedy that breach within 30 days of that party being notified in writing of the breach; or
- (b) an order is made or a resolution is passed for the winding up of the other party, or circumstances arise which entitle a court of competent jurisdiction to make a winding-up order in relation to the other party; or
- (c) an order is made for the appointment of an administrator to manage the affairs, business and property of the other party, or documents are filed with a court of competent jurisdiction for the appointment of an administrator of the other party, or notice of intention to appoint an administrator is given by the other party or its directors or by a qualifying floating charge holder (as defined in paragraph 14 of Schedule B1 to the Insolvency Act 1986); or
- (d) a receiver is appointed of any of the other party's assets or undertaking, or if circumstances arise which entitle a court of competent jurisdiction or a creditor to appoint a receiver or manager of the other party, or if any other person takes possession of or sells the other party's assets; or
- (e) the other party makes any arrangement or composition with its creditors, or makes an application to a court of competent jurisdiction for the protection of its creditors in any way; or
- (f) the other party ceases, or threatens to cease, to trade; or
- (g) the other party takes or suffers any similar or analogous action in any jurisdiction in consequence of debt.

15.3 On any termination of this agreement for any reason or expiry of the Term:

- (a) each party shall as soon as reasonably practicable return or destroy (as directed in writing by the other party) all Data, information, software, and other materials provided to it by the other party in connection with this agreement including all materials containing or based on the other party's Confidential Information, except for one copy that it may use for audit purposes only, and subject to the confidentiality obligations in clause 11 and except, in the case of the Customer only, for all Processed Data delivered up to the date of termination;
- (b) if the Customer elects for destruction rather than return of the materials, the Supplier shall as soon as reasonably practicable ensure that all Relevant Data is deleted from the Supplier System; and

- (c) the Customer shall pay all reasonable expenses incurred by the Supplier in returning or disposing of the Customer Data.
- 15.4 If the Customer elects for return rather than destruction of the materials under and the Supplier receives, no later than ten days after the effective date of the termination or expiry of this agreement, a written request for the delivery to the Customer of the most recent back-up of the Customer Data, the Supplier shall use reasonable commercial efforts to fulfil such request within 30 days of its receipt, provided that the Customer has, at that time, paid all fees and Charges outstanding at, and resulting from, termination (whether or not due at the date of termination). If the Customer makes no such election within that ten-day period, the Supplier may destroy or otherwise dispose of any of the Customer Data in its possession. In any instance, all customer data held by Aerona will be destroyed within 90 days of contract termination.
- 15.5 Each party shall provide written confirmation of compliance with clause 15.3(a) and, in the case of the Supplier only, clause 15.3(b) (in the form of a letter signed by its Authorised User no later than 14 days after termination of this agreement).
- 15.6 If a party is required by any law, regulation, or government or regulatory body to retain any documents or materials that it would otherwise be required to return or destroy under clause 15.3, it shall notify the other party in writing of that retention, giving details of the documents or materials that it must retain. That party shall not be in breach of clause 15.3 with respect to the retained documents or materials, but clause 11 shall continue to apply to them; and
 - (a) the accrued rights of the parties as at termination, or the continuation after termination of any provision expressly stated to survive or implicitly surviving termination, shall not be affected or prejudiced.

16. FORCE MAJEURE

The Supplier shall have no liability to the Customer under this agreement if it is prevented from or delayed in performing its obligations under this agreement, or from carrying on its business, by acts, events, omissions or accidents beyond its reasonable control, including, without limitation, strikes, lock-outs or other industrial disputes (whether involving the workforce of the Supplier or any other party), failure of a utility service or transport or telecommunications network, act of God, war, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, breakdown of plant or machinery, fire, flood, storm or default of suppliers or sub-contractors, provided that the Customer is notified of such an event and its expected duration.

17. WAIVER

17.1 A waiver of any right under this agreement is only effective if it is in writing and it applies only to the party to whom the waiver is addressed and to the circumstances for which it is given.

17.2 Unless specifically provided otherwise, rights arising under this agreement are cumulative and do not exclude rights provided by law.

18. SEVERANCE

18.1 If any provision (or part of a provision) of this agreement is found by any court or administrative body of competent jurisdiction to be invalid, unenforceable or illegal, the other provisions shall remain in force.

18.2 If any invalid, unenforceable or illegal provision would be valid, enforceable or legal if some part of it were deleted, the provision shall apply with whatever modification is necessary to give effect to the commercial intention of the parties.

19. ENTIRE AGREEMENT

19.1 This agreement, and any documents referred to in it, constitute the whole agreement between the parties and supersede any previous arrangement, understanding or agreement between them relating to the subject matter they cover.

19.2 Each of the parties acknowledges and agrees that in entering into this agreement it does not rely on any undertaking, promise, assurance, statement, representation, warranty or understanding (whether in writing or not) of any person (whether party to this agreement or not) relating to the subject matter of this agreement, other than as expressly set out in this agreement.

20. ASSIGNMENT

20.1 The Customer shall not, without the prior written consent of the Supplier, assign, transfer, charge, sub-contract or deal in any other manner with all or any of its rights or obligations under this agreement.

20.2 The Supplier may at any time assign, transfer, charge, sub-contract or deal in any other manner with all or any of its rights or obligations under this agreement.

21. NO PARTNERSHIP OR AGENCY

Nothing in this agreement is intended to or shall operate to create a partnership between the parties, or authorise either party to act as agent for the other, and neither party shall have the authority to act in the name or on behalf of or otherwise to bind the other in any way (including, but not limited to, the making of any representation or warranty, the assumption of any obligation or liability and the exercise of any right or power).

22. THIRD PARTY RIGHTS

This agreement does not confer any rights on any person or party (other than the parties to this agreement and, where applicable, their successors and permitted assigns) pursuant to the Contracts (Rights of Third Parties) Act 1999.

23. NOTICES

23.1 Any notice required to be given under this agreement shall be in writing and shall be delivered by hand or sent by pre-paid first-class post or recorded delivery post to the other party at its address set out in this agreement, or such other address as may have been notified by that party for such purposes, or sent by fax to the other party's fax number as set out in this agreement.

23.2 A notice delivered by hand shall be deemed to have been received when delivered (or if delivery is not in business hours, at 9 am on the first business day following delivery). A correctly addressed notice sent by pre-paid first-class post or recorded delivery post shall be deemed to have been received at the time at which it would have been delivered in the normal course of post. A notice sent by fax shall be deemed to have been received at the time of transmission (as shown by the timed printout obtained by the sender).

24. GOVERNING LAW AND JURISDICTION

24.1 This agreement and any disputes or claims arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) are governed by, and construed in accordance with, the law of Northern Ireland.

24.2 The parties irrevocably agree that the courts of Northern Ireland have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with this agreement or its subject matter or formation (including non-contractual disputes or claims).

This agreement has been entered into on the date stated at the beginning of it.

24.3 The Customer shall be automatically enrolled in our referral scheme for the duration of their subscription. No details will be shared with third parties.

This agreement has been entered into on the date the Customer accepted the terms.

Schedule One Back Up Policy

Purpose

The technology used to facilitate data backups at Aerona software is to provide a real time backup of customer data for disaster recovery purposes only. The backup service allows for data to be stored off site in Amazon Web Services.

Scope

The service and hence this policy has been designed and implemented with disaster recovery/business continuity (i.e. the ability to recover at a selected point in time from the previous 35 days) in the event of a partial or total loss of data) as a key deliverable and is not therefore designed as a method of archiving material for extended periods of time. The 'data' backups cover all customer data and files managed by Aerona Software.

- A full backup of all data is performed each night
- Full backups are retained for 35 days.
- Point and time restore is available for these backups within the last 35 days
- Including Customer data, customer files are also copied over in real time. So when they make a change to one of their files it is transferred across to AWS S3 storage.
- All backups are stored on AWS S3 storage.
- All other files related to customers are backed up on AWS S3 storage.

Schedule Three Employee Access Policy

We regard your data as private and confidential to your practice and patients.

Everyone within Aerona has an important role to play in maintaining the security of information, each with their own specific tasks, and responsibilities. Aerona staff do not have physical access to our servers. Electronic Access to the servers and services is restricted to a core set of approved Aerona users and permissions are set using the AWS Identity and Access Management (IAM).

Aerona staff will only access your data to assist with support, to resolve customer issues and as outlined in our terms & conditions.

Aerona staff cannot see your password.

We support staff efforts to secure information through continual staff training and awareness activities.

Schedule Four Security & Privacy Policy

Maintaining the security, integrity, and confidentiality of your data is our top priority. Below are some of the ways we implement security at Aerona

Physical Security

Aerona uses Amazon Web Services (AWS) to host its servers. We store your data according to what best fits the compliance for your data. All EU data will be stored in EU servers under GDPR and UK data will be stored in UK servers.

AWS adheres to multiple security standards including ISO 27001 certified and is PCI compliant this ensures exceptional levels of security, all the time.

To see a comprehensive list of AWS compliance programs use the link below

<https://aws.amazon.com/compliance/programs/>

AWS Firewall Manager is used to administer and maintain the AWS Web Application Firewall on the site.

All data is stored in AWS S3 and is backed by the Amazon S3 Service Level agreement. The data is further protected using the Amazon S3 versioning facility.

To find out more about AWS security see here: <https://aws.amazon.com/security/>

Application and Data Security

The following security measures are in place at the application level:

All passwords are encrypted in the Database.

All web applications use a TLS 1.2 128 bit key and are not accessible via a non-secure connection.

We provide encryption in transit using HTTPS by default on all Aerona domains.

All Java Applet jars are signed with a security certificate.

The login process for AeronaClinic requires three pieces of data, Username, Password and Practice PIN.

Aerona performs resets daily to ensure any active sessions on the system are reset.

Users are automatically logged out after 1 hour of inactivity and 15 minutes of inactivity on the Portals.

In relation to APIs a Token Based Authentication system is used to validate requests. Tokens are valid for one hour after creation. A user can only make 300 requests to the APIs in a 15minute time frame.

Practice Level Security

Aerona provides the following features to allow you to enhance security at a practice level:

Users can change their own passwords.

No users can see other user's passwords.

There are different levels of access for the different roles within a practice.

Users can be restricted on the times they can log-in to the system.

We can also confirm that we are fully compliant and meet the standards of the EU Data Regulations, May 2018.

Schedule Five Data Processing Policy

1. DATA PROTECTION OBLIGATIONS

- 1.1 To the extent that the provision of the Services involves the processing of Personal Data and/or Sensitive Personal Data by the Supplier, the Supplier agrees that:
- 1.1.1 For any Personal Data and/or Sensitive Personal Data processed by Supplier in connection with the Services, the parties acknowledge that Customer shall be the Data Controller and the Supplier shall be the Data Supplier;
 - 1.1.2 The Supplier shall implement the Technical and Organisational Security Measures and all other relevant and appropriate measures (having regard to the state of the art and the cost of implementation) to ensure a level of security appropriate to the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage to Personal Data and/or Sensitive Personal Data, and to reflect the nature of the Personal Data and/or Sensitive Personal Data to be protected. The Supplier shall maintain reasonable operating standards and security procedures, and shall use all reasonable efforts to secure Personal Data and/or Sensitive Personal Data through the use of appropriate network security measures and encryption technologies.
 - 1.1.3 Supplier shall notify Customer of any actual or anticipated breaches of its security (including where the Personal Data and/or Sensitive Personal Data have been put at risk of any unauthorised or accidental access) which are likely to or actually affect the Personal Data and/or Sensitive Personal Data or its security ("**Information Security Breach**") immediately, and at least within 24 hours of, becoming aware of such breaches. Upon discovery of such an Information Security Breach, the Supplier will (i) investigate, remediate and mitigate the effects of the Information Security Breach; (ii) provide the Customer with assurances reasonably satisfactory to the Customer that such Information Security Breach will not recur; and (iii) take such remedial measures as it is required to to comply with the PDPR.
 - 1.1.4 the Personal Data and Sensitive Personal Data are confidential in nature and Supplier shall, unless otherwise directed by Customer:
 - (a) process the Personal Data and/or Sensitive Personal Data (on behalf of Customer) exclusively for the provision of the Services but for no other purposes whatsoever and in accordance with the terms of this Agreement, the Principal Agreement and all applicable data protection legislation;
 - (b) process the Personal Data and/or Sensitive Personal Data solely in accordance with the instructions of Customer and comply in full with any instructions of the Customer regarding Personal Data and/or Sensitive Personal Data;

- (c) take all reasonable steps to ensure that each of its employees and/or agents engaged in processing the Personal Data and/or Sensitive Personal Data will be informed of the confidential nature of the Personal Data and/or Sensitive Personal Data and will comply with the provisions of this Agreement, the Principal Agreement and all applicable data protection legislation;
 - (d) take all reasonable steps to ensure that neither Supplier nor any of its employees or agents publish, disclose or divulge Personal Data and/or Sensitive Personal Data to any third party unless otherwise required by this Agreement or as directed in writing to do so by Customer; and
 - (e) not (and shall ensure that their employees, agents and temporary contractors shall not) process nor transfer any Personal Data and/or Sensitive Personal Data outside the EEA without the prior written consent of Customer;
- 1.1.5 The Supplier may disclose Personal Data and/or Sensitive Personal Data only to those of its employees (in accordance with the Employee Access Policy set out in Schedule 2 of this Agreement), agents and temporary contractors as it reasonably considers necessary for the administration of the Services on similar terms to those set out in this Agreement;
- 1.1.6 At all times applicable to the Supplier's obligations under this Agreement to the Customer, the Supplier will, at no cost to the Customer, maintain cyber insurance and provide the Customer with a copy of the relevant insurance certificate.
- 1.1.7 At the choice of the Customer, the Supplier shall securely delete or return to the Customer all the Personal Data and/or Sensitive Personal Data which it holds at the end of the provision of the Services. In addition, if requested by the Customer at any time during the term of this Agreement or the Principal Agreement, the Supplier will, at the choice of the Customer, securely delete or return to the Customer specified Personal Data and/or Sensitive Personal Data which it holds.
- 1.1.8 Supplier shall (and shall procure that its agents shall) promptly notify Customer about:
 - (a) any legally binding request for disclosure of the Personal Data and/or Sensitive Personal Data by a law enforcement or other applicable authority unless otherwise prohibited by applicable law;
 - (b) all requests received directly from the Data Subjects without responding to that request, unless they have been otherwise authorised by Customer to do so; and
 - (c) shall assist Customer in taking any actions deemed necessary or appropriate to deal with complaints or

allegations of or in connection with a failure to comply with the PDPR;

- 1.1.9 Customer may, upon giving Supplier reasonable notice, carry out an audit in relation to the Services to satisfy itself that Supplier is complying with the PDPR in respect of the Services and Supplier shall (and shall ensure that their agents shall) if requested by Customer, promptly provide a detailed, written description of the Technical and Organisational Security Measures implemented PROVIDED HOWEVER that any information obtained by Customer in connection with or in the course of any such audit and any written description of the Technical and Organisational Security Measures shall be maintained by Customer in the strictest confidence, that such audit shall not require the Processor to breach the PDPR in respect of other customers' Data, shall be used solely for the purposes of determining whether Supplier is complying with its obligations as a Data Supplier under the PDPR and shall not be used or disclosed for any other purpose. The Supplier will cooperate with any such audit carried out by the Customer, or any audit carried out by any relevant authority, and make available all information necessary to demonstrate compliance with its data processing obligations.
- 1.2 The Supplier shall deal promptly and properly with all inquiries from the Customer relating to the processing by the Supplier of the Personal Data and/or Sensitive Personal Data and provide any relevant documentation requested from the Customer in respect of this processing.
- 1.3 The Supplier shall provide assistance and support, and assist and support the Customer in the event of an investigation by a data protection regulator or similar authority, if and to the extent that such investigation relates to the collection, maintenance, use, processing or transfer of Personal Data and/or Sensitive Personal Data under this Agreement.
- 1.4 In the event that the Supplier is unable to comply with its obligation under this Agreement, the Supplier shall immediately notify the Customer, and the Customer may take any one or more of the following actions: (i) suspend the transfer of Personal Data and/or Sensitive Personal Data to the Supplier, (ii) require the Supplier to cease processing Personal Data and/or Sensitive Personal Data, (iii) demand the return or destruction of Personal Data and/or Sensitive Personal Data; or (iv) immediately terminate this Agreement and/or the Principal Agreement.
- 1.5 The Customer agrees that it will comply with its obligations as a Data Controller under the PDPR.