VERBO END USER LICENCE AGREEMENT & DATA PROCESSING AGREEMENT

1. VERBO END USER LICENCE AGREEMENT

These Terms and Conditions (Terms) govern your use of our Verbo website (Site) and form a binding contractual agreement between the user (You) and Verbo (Us).

These Terms are important and You should ensure that you read them carefully and contact Us at hello@verboapp.co.uk if You have any questions before using our products or engaging our services.

These Terms constitute the entire and only agreement between You and Us and supersede all prior conduct, agreements, representations and understandings.

1. ACCEPTANCE OF TERMS
   - 1.1. By accessing, downloading, using or saving any part of the products and services offered on our Site, You agree to be bound by these Terms, which You acknowledge that You have read and understood.
   - 1.2. We may change all or part of these Terms at any time. If we do, the new terms and conditions will be posted on our Site. Your continued use of the Site will constitute your acceptance of any changes. If You object to any changes to the Terms, your only remedy is to immediately discontinue your use of the products and/or services.

2. GENERAL DISCLAIMER
   - 2.1. The products and services on our Site are intended for education and information purposes only. Nothing on this Site, or any of the content provided to You by Us during our provision of the products and/or services offers any guarantee of improvement in any condition, medical or otherwise.
   - 2.2. Any testimonials and examples within our marketing materials are not to be taken as a guarantee that You will achieve the same or similar results.
   - 2.3. We do not guarantee the completeness or accuracy of material used on our Site, nor that it will remain up to date.
   - 2.4. We do not guarantee that the Site will remain available.
   - 2.5. We are not responsible for any network issues relating to access of our Site. Please refer to our Network Requirements Policy for information.

3. REGISTERING YOUR DETAILS
   - 3.1. Before you access our products and/or services, You must register a user account with Us.
   - 3.2. Your user account must be registered using the email address and/or log in details provided to You by the organisation who pays the Verbo licence fee. This may be your employer, another organisation that has purchased a licence for your employer to use, your setting (if You are a pupil or a young person), or the setting of the person you parent or care for.
   - 3.3. You must provide accurate, complete and up-to-date registration information, as requested, and it is your responsibility to inform Us of any changes to your registration information.
   - 3.4. We may at any time request a form of identification to verify your identity.
   - 3.5. If You are a registered user of this this Site, You acknowledge and agree that:
   - 3.6. You are solely responsible for protection and confidentiality of any password or user identification that may be issued to You from time to time (Password);

3.7. You will not reveal (or cause to be revealed through any act or omission) your Password to any other person;

3.8. You will immediately notify Us if your Password is lost or becomes known to any other person;

3.9. You are solely responsible for all access to and use of this Site via your Password, whether such access or use is by You or any other person;

3.10. Any information or feedback You provide to Us relating to the Site, immediately becomes our property;

3.11. We will treat any personal information You provide Us strictly in accordance with our Privacy Policy;

3.12. You must ensure the security and confidentiality of your registration details, including any username and/or Password. You must notify Us immediately if You become aware of any unauthorised use of your registered details;

3.13. The Site access You have been given is for one user only. You will not let any other person use your Password to access the Site. We reserve the right to cancel your access if we have reason to believe You have shared your username and/or Password.

4. CONFIDENTIALITY

4.1. By using our products and/or services and our Site, You agree to respect our confidential and proprietary information and ideas, (collectively, **Confidential Information**) and specifically, You agree:

4.1.1. That all materials and information provided to You by Us, whether via the Site or by other means, are our confidential, proprietary information and intellectual property and belong solely and exclusively to Us;

4.1.2. That You may not share any Confidential Information with any other party except as authorised by Us;

4.1.3. That if You violate, or threaten to violate, the obligations contained in this clause, we will be entitled to, among other things, injunctive relief to prohibit such violations.

4.2. This clause shall survive termination of these Terms.

5. INTELLECTUAL PROPERTY

5.1. All material on our Site, including, but not limited to, video, audio and/or written text, course content, graphics, layout and appearance, information architecture and coding (**Content**), constitutes our Intellectual Property.

5.2. All the Intellectual Property Rights contained on our Site are reserved.

5.3. You may access, download, browse, save or print our Content for personal use and for non-commercial purposes only. Any other purpose constitutes a violation of our Intellectual Property Rights and is strictly prohibited.

5.4. You acknowledge that You do not acquire any ownership rights by using the Site or our Content.

5.5. You may only reference our Content in accordance with these Terms and where You do so, You must clearly acknowledge our Site.

5.6. Any trademarks, logos, and service marks displayed on our Site are the registered and/or unregistered trademarks of Verbo. The trademarks whether registered or unregistered, may not be used in connection with any product or service that does not belong to Verbo.

5.7. Nothing contained on this Site should be construed as granting, by implication, estoppel or otherwise, any licence or right to use any trademark without our express written permission.

5.8. You agree that damages may be an inadequate remedy to a breach of these Terms and acknowledge that we will be entitled to seek injunctive relief if such steps are necessary to prevent violations of our Intellectual Property Rights.

5.9. This clause shall survive termination of these Terms.

6. LICENCE

6.1. The term of your licence shall be determined by the organisation responsible for paying the licence fees.

6.2. Where You have access to the Site under a paid for licence, You may, during the term of your licence, access and browse the Site and You may download, save or print the Content from the Site for your personal use and for non-commercial purposes.

6.3. You agree not to copy, share, resell, modify, edit, reproduce or attempt to reverse engineer any of the Content on the Site at any time.

6.4. You may not take any action that causes, or may cause, damage to the Site or impairment of the performance, accessibility or availability of the Site at any time.

6.5. You agree not to use the Site or any of the Content for any unlawful, illegal or fraudulent purpose or activity.

6.6. Any use of the Site or the Content for any purpose not stipulated in these Terms is strictly prohibited.

7. FREE TRIAL PERIOD

7.1. During a free trial period, You may access the Site and browse the Content only. You may not download, save or print any of the Content during a free trial period.

7.2. Except for the licence granted in 6.2 above, these Terms shall apply to You in full during any free trial period.

7.3. You must cease use of the Site and the Content upon expiration of any free trial period.

8. RIGHT TO SUSPEND AND TERMINATE

8.1. We reserve the right to suspend or terminate your use of the Site, at our sole discretion, and with immediate effect, if You breach any of these Terms, at any time. This may also affect the rights of your employer, subject to the terms of our agreement with them.

8.2. You acknowledge that your access to our Site is linked to your employment and that your employer is responsible for paying a licence fee. You must cease all use of our Site upon suspension or termination of your employment.

8.3. Your right to use the Site and any Content which you have downloaded, saved or printed, will immediately cease upon termination of the licence under which you have been granted access to Verbo. This licence may be with your employer, another organisation that has purchased a licence for your employer to use, your setting (if You are a pupil or a young person), or the setting of the person you parent or care for. It is your responsibility to ensure that the organisation continues to have a valid licence in place while You continue to access the Site or use any of its Content.

9. LIMITED LIABILITY

9.1. The disclaimers, liability limitations and indemnities within these Terms do not exclude rights that by law may not be excluded.

9.2. We do not make any express or implied representation or warranty about, nor shall be liable, in contract, tort (including negligence) or otherwise, for any direct, indirect, special or consequential loss, damages or reliance in connection with any of our Site or the Content.

9.3. In no event will we be liable for any damages whatsoever, including but not limited to any direct, indirect, special, consequential, punitive or incidental damages, or damages for loss of use, profits, data or other intangibles, or the cost of procurement of substitute products or services arising out of or related to the use, inability to use, unauthorised use, performance or non-performance of, or reliance upon our Site or the Content.

9.4. These limitations and terms include (but are not restricted to) loss or damage You might suffer as a result of:

9.4.1. Reliance on the completeness, accuracy, suitability or currency of information, Content, our products or services, irrespective of any verifying measures taken by Us (including third party material and advertisements);

9.4.2. Failure of performance, error, omission, interruption, deletion, defect, failure to correct defects, delay in operation or transmission, computer virus or harmful component, loss of data, communication line failure, unlawful third-party conduct, theft, destruction, alteration or unauthorised access to records;

9.4.3. Accessing websites or servers maintained by other organisations through links on our Site. Links are provided for convenience only. We do not endorse linked websites, nor their products and services and You access them at your own risk.

10. YOUR INDEMNITY

10.1. You indemnify us from all actions, suits, claims, demands, liabilities, costs, expenses, loss and damage (including legal fees on a full indemnity basis) incurred or suffered by You or Us as a direct or indirect consequence of using or attempting to use our Site or our Content, or for any breach by You of these Terms.

10.2. We are not responsible for, and expressly disclaim all liability to the fullest extent permitted by law, for damages of any kind arising out of use, reference to, or reliance on any information contained within our Site, or through use of our Content, products or services.

11. NO ASSIGNMENT, TRANSFER OR SUB-LICENCE

11.1. You may not transfer, assign or sub-licence your user access to any other person at any time.

11.2. Notwithstanding the permissions granted in clause 12 below, these Terms do not grant any third-party licences to use our Site or the Content.

11.3. We may assign or transfer our obligations under these Terms at any time.

12. ADMIN USERS

12.1. Different users of the Verbo Site will be granted different levels of access. Some users will be given Admin User status. If You have been given access to our Site as an Admin User, You will be able to create Verbo account log-ins for pupils and young persons who attend the organisation where you work, and to whom Your organisation provides SEN services. You may also be able to create account log-ins for the parents or carers of the pupils or young persons to whom Your organisation provides the SEN services. You will know which access level You have from Your user description on the Site, but the Admin User levels are also detailed in Appendix A to this Verbo End User Licence Agreement.

12.2. In all cases, any users for whom You create Verbo log-ins, must also agree and accept the terms of this End User License Agreement.

12.3. If You are an Admin User, You must liaise with the Verbo setting Lead User in Your organisation (or their successor) and keep a record of all other Users who You create Verbo account log-ins for. This record must be maintained and kept current, providing details of all Users who are linked to Your organisation and any who have ceased to be linked to Your organisation, (e.g. pupils and their parents or carers who change settings), whether or not those Users intend to continue accessing Verbo in a new organisation or not.

12.4. The rights granted by this clause 12 shall be subject always to the terms of this Agreement.

13. APPLICABLE LAW

13.1. These Terms shall be construed in accordance with and governed by the laws of England and Wales. You consent to the exclusive jurisdiction of the courts of England to determine any matter or dispute which arises between us.

14. YOUR FEEDBACK

14.1. We welcome enquiries or feedback on our Site. We shall treat any information You provide Us as non-proprietary and non-confidential.

14.2. Any modifications or improvements to the Content or Site that we incorporate as a result of your feedback shall immediately become part of our Content.

14.3. If You have questions or comments regarding this Site or the products and services we provide, please email us at hello@verboapp.co.uk

Appendix A to Verbo End User Licence Agreement

User Admin Level Access

When Verbo users are signed up to access the platform, they are allocated a user level.

This may be a basic level, or it may include some administrative rights attached.

Where users have any administrative rights, they are able to:

- Add pupils
- Add a parent or carer
- Complete a screener
- Select and outcome targets
- Access content (download and watch)
- Access an environment audit

Other features on the platform can only be accessed by users with administrative rights. The table below provides details of those additional features and which user admin levels are able to access them:

User Admin Level	Access	What the User Cannot Do
The Verbo Team (Master Admin)	Can see all users and activity Can set up all types of user Can offer calls in the in app calling calendar Can edit local information Can filter and pull data at wider geographical level across all users Add any user onto the platform Set call quota for clinical admin Set licence numbers for master admin Can add and edit all content	
Speech & Language Therapist(s)	Can see users and activity in local regional area Can offer calls in the in app calling calendar Can book calls with Verbo SaLT Can edit local information Can filter and pull data at wider geographical level across settings they are working in Can set up and edit multiple settings (linked to agreed number on contract)	Can't add or edit content Unable to view settings they are not working in

	Can be linked to more than one setting setting	
Multi-setting User - a person who has oversight of a collection of settings e.g. LA lead, Exec Head of Multi Academy Trust	Can see users in local regional area Can edit local information Can filter and pull data at wider geographical level Add/edit settings within a given number of licenses Can access all content Can turn off content	Can't add or edit content Unable to view settings outside geographical region
Verbo setting Lead - e.g. SENCo/Deputy Head	Can see all users in an individual setting Can book calls within app Can filter and pull data for individual setting Can access all content Can allocate lead admin to specific pupils	Can't add or edit content
Teaching/Support Staff	Can add and edit pupils Can add and edit parent log ins Can see pupils they are assigned to by senior admin	Can't add or edit content Cannot see activity completed by other staff in their setting

2. DATA PROCESSING AGREEMENT

This agreement shall be binding on both parties subject only to where there is formal contract with consideration in place between said parties as required under Article 28(3) of the UK GDPR

Status of the Controller

1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA. A Party may act as:

    a. "Controller" in respect of the other Party who is "Processor"
    b. "Processor" in respect of the other Party who is "Controller";
    c. "Joint Controller" with the other Party;
    d. "Independent Controller" of the Personal Data where there other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

1. Where one Party is Controller and the other Party its Processor
2. Where a Party is a Processor, the only processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.
3. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation
4. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

    a. a systematic description of the envisaged Processing and the purpose of the Processing;
    b. an assessment of the necessity and proportionality of the Processing in relation to the Services;
    c. an assessment of the risks to the rights and freedoms of Data Subjects; and
    d. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

5. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

    a. Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before Processing the Personal Data unless prohibited by Law;
    b. ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the

Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

i. nature of the data to be protected;
ii. harm that might result from a Data Loss Event;
iii. state of technological development; and
iv. cost of implementing any measures;

c. ensure that:
   i. the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data)*);
   ii. it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
      A. are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);
      B. are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
      C. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
      D. have undergone adequate training in the use, care, protection and handling of Personal Data;
d. not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
   i. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;
   ii. the Data Subject has enforceable rights and effective legal remedies;
   iii. the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
   iv. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and
e. at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

6. Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:
   a. receives a Data Subject Request (or purported Data Subject Request);
   b. receives a request to rectify, block or erase any Personal Data;

c. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
d. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
e. receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
f. becomes aware of a Data Loss Event.

7. The Processor's obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller in phases, as details become available.
8. Taking into account the nature of the Processing, the Processor shall provide the Controller with reasonable assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:
    a. the Controller with full details and copies of the complaint, communication or request;
    b. such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;
    c. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
    d. assistance as requested by the Controller following any Data Loss Event; and/or
    e. assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

9. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
    a. the Controller determines that the Processing is not occasional;
    b. the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or
    c. the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

10. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
11. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
12. Before allowing any Sub-processor to Process any Personal Data related to the Contract, the Processor must:
    a. notify the Controller in writing of the intended Subprocessor and Processing;

b. obtain the written consent of the Controller;
c. enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and
d. provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

13. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
14. The Relevant Authority may, at any time on not less than 30 Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).
15. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than 30 Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.
16. The Parties shall only provide Personal Data to each other:
    a. to the extent necessary to perform their respective obligations under the Contract;
    b. in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the GDPR); and
    c. where it has recorded it in Annex 1 *(Processing Personal Data).*

17. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the GDPR.
18. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 GDPR and shall make the record available to the other Party upon reasonable request.
19. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract ("**Request Recipient**"):

    a. the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
    b.
    c. where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

i. promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
ii. provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

20. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:
    a. do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
    b. implement any measures necessary to restore the security of any compromised Personal Data;
    c. work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
    d. not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

21. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data)*.
22. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.
23. Notwithstanding the general application of paragraphs 2 to 15 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs16 to 27 of this Joint Schedule 11.

Annex 1 - Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

1. The contact details of the Relevant Authority's Data Protection Officer or designated Responsible Manager must be provided to the Processor upon request if required
   1.1. The contact details of the Supplier's Data Protection Officer are: David Waters (huh-tr.ig@nhs.net)
   1.2. The Processor shall comply with any further written instructions with respect to Processing by the Controller.
   1.3. Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	The Relevant Authority is Controller and the Supplier is Processor The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: *The scope of Personal Data for which the purposes and means of the Processing by the Supplier is determined by the Relevant Authority* • Adult name* • Adult job role* • Adult email address* • Name of setting/place of work* • Child name* • Child DoB* • Key Stage* • Class • Year Group • SEN Support Level • Postcode • Name of Teacher • Name of support staff • Parent/carer name • Parent/carer email *Mandatory Data

Processor Data Protection Registration	Z5917319 (Tier 3)
Duty of Confidence	All NHS workers are contractually bound by the duty of confidence
Lawful Basis for processing	6(1)(a) Consent 9(2)(a) Direct Consent

Duration of the Processing	The duration of the processing will be for the full term of the contract, it will commence upon signature of the contract
Nature and purposes of the Processing	Within the platform the organisation have the ability to: • Screen a child's communication needs • Allocate individual targets • Access resources to work towards targets • rack progress towards targets
Type of Personal Data	• Adult name* • Adult job role* • Adult email address* • Name of setting/place of work* • Child name* • Child DoB* • Key Stage* • Class • Year Group • SEN Support Level • Postcode • Name of Teacher • Name of support staff • Parent/carer name • Parent/carer email *Mandatory Data
Categories of Data Subject	Setting Staff, Pupils (Patients), Parents/Guardians, Assigned health and education professionals

Plan for return and destruction of the data once the Processing is complete UNLESS requirement under law to preserve that type of data	Verbo Personal Confidential Data retention policy aligns to the NHS Records Management Code of Practice Records Management Code of Practice - NHS Transformation Directorate (england.nhs.uk)

1. Undertakings of both Parties

1.1 The Supplier and the Relevant Authority each undertake that they shall:

a. report to the other Party every Quarter.
   i. the volume of Data Subject Request (or purported Data Subject Requests) from Data Subjects (or third parties on their behalf);
   ii. the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
   iii. any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;
   iv. any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
   v. any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law, that it has received in relation to the subject matter of the Contract during that period;
b. notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
c. provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
d. not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, save where such disclosure or transfer is specifically authorised under the Contract or is required by Law). For the avoidance of doubt to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;
e. request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;
f. ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

g. take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
   i. are aware of and comply with their 's duties under this Annex 2 (Data Sharing Agreement) and those in respect of Confidential Information
   ii. are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;
   iii. have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Law;

h. ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:
   i. nature of the data to be protected;
   ii. harm that might result from a Data Loss Event;
   iii. state of technological development; and
   iv. cost of implementing any measures;
   v. ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Law, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and
   vi. ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

1.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Law and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Law to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations

2. Data Protection Breach

2.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the Relevant Authority and its advisors with:

a. sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;
b. all reasonable assistance, including:

   i. co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and

recovering the compromised Personal Data and compliance with the applicable guidance;

ii. co-operation with the other Party including taking such reasonable steps as are directed by the Relevant Authority to assist in the investigation, mitigation and remediation of a Personal Data Breach;

iii. co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

iv. providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

2.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

a. the nature of the Personal Data Breach;
b. the nature of Personal Data affected;
c. the categories and number of Data Subjects concerned;
d. the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;
e. measures taken or proposed to be taken to address the Personal Data Breach; and
f. describe the likely consequences of the Personal Data Breach.

3. Audit

3.1 The Supplier shall permit:

a. the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Law; and/or
b. the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

3.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

4. Impact Assessments

4.1 The Parties shall:

a. provide all reasonable assistance to each other to prepare any data protection impact assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and
b. maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 GDPR.

5. ICO Guidance

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

6. Liabilities for Data Protection Breach

[Guidance: This clause represents a risk share; you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

6.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("Financial Penalties") then the following shall occur:

a. if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;
b. if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

c. if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (*Resolving disputes*).

6.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.
6.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

a. if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;
b. if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and
c. if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.

6.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Relevant Authority.

9. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Control Memorandum of Understanding*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 (*Ending the contract*).

10. Sub-Processing

10.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

a. carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is

required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

b. ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Law.

11. Data Retention

The Parties agree to erase 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 Law 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 Law and its privacy policy.