DATA PROTECTION ADDENDUM

IMPORTANT

A. If a data processing agreement is in force between the Supplier and the Customer at the Order Acceptance for the duration of our Agreement, the terms of that data processing agreement shall apply.

B. If a data processing agreement is in force between the Supplier and the Customer at the Order Acceptance (whether or not for the duration of our Agreement) but that data processing agreement is terminated or expires then, from the date of termination or expiry, the Supplier and the Customer agree to be bound by the terms of this Data Protection Addendum.

C. If there is no data processing agreement in force between the Supplier and the Customer at the Order Acceptance, the terms of this Data Protection Addendum shall apply to our Agreement.

1 Application and definitions

1.1 In this Data Protection Addendum defined terms shall have the same meaning, and the same rules of interpretation shall apply as in the remainder of our Agreement. In addition in this Data Protection Addendum the following definitions have the meanings given below:

Applicable Law means applicable laws of the European Union (EU), the European Economic Area (EEA) or any of the EU or EEA's member states from time to time together with applicable laws in the United Kingdom from time to time*;*

Appropriate Safeguards means such legally enforceable mechanism(s) for Transfers of Personal Data as may be permitted under Data Protection Laws from time to time;

Controller has the meaning given to that term in Data Protection Laws;

Data Protection Laws means all Applicable Laws relating to the processing, privacy and/or use of Personal Data, as applicable to either party or the Services, including the following laws to the extent applicable in the circumstances:

(a) the GDPR;

(b) the Data Protection Act 2018;

(c) any laws which implement any such laws; and

(d) any laws which replace, extend, re-enact, consolidate or amend any of the foregoing**[** (including where applicable, the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of the European Union (Withdrawal) Act 2018 as modified by applicable domestic law from time to time**]**);

Data Protection Losses means all liabilities, including all:

(a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and

(b) to the extent permitted by Applicable Law:

(i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority;

(ii) compensation which is ordered by a Supervisory Authority to be paid to a Data Subject; and

(iii) the reasonable costs of compliance with investigations by a Supervisory Authority;

Data Subject has the meaning given to that term in Data Protection Laws;

Data Subject Request means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;

GDPR means the General Data Protection Regulation, Regulation (EU) 2016/679;

International Recipient means the organisations, bodies, persons and other recipients to which Transfers of Protected Data are prohibited under paragraph 7.1 without the Customer's prior written consent;

SaaS Terms means the latest version of the Supplier's master SaaS terms available at [*insert URL*], as Updated from time to time;

Onward Transfer means a Transfer from one International Recipient to another International Recipient;

Personal Data has the meaning given to that term in Data Protection Laws;

Personal Data Breach means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;

processing has the meanings given to that term in Data Protection Laws (and related terms such as **process** have corresponding meanings);

Processing Instructions	has the meaning given to that term in paragraph 3.1.1;
Processor	has the meaning given to that term in Data Protection Laws;
Protected Data	means Personal Data in the Customer Data;
Sub-Processor	means another Processor engaged by the Supplier for carrying out processing activities in respect of the Protected Data on behalf of the Customer;
Supervisory Authority	means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws;
Transfer	bears the same meaning as the word 'transfer' in Article 44 of the GDPR. Without prejudice to the foregoing, this term also includes all Onward Transfers. Related expressions such as **Transfers**, **Transferred** and **Transferring** shall be construed accordingly; and

2 Processor and Controller

2.1 The parties agree that, for the Protected Data, the Customer shall be the Controller and the Supplier shall be the Processor.

2.2 To the extent the Customer is not sole Controller of any Protected Data it warrants that it has full authority and authorisation of all relevant Controllers to instruct the Supplier to process the Protected Data in accordance with our Agreement.

2.3 The Supplier shall process Protected Data in compliance with:

2.3.1 the obligations of Processors under Data Protection Laws in respect of the performance of its and their obligations under our Agreement; and

2.3.2 the terms of our Agreement.

2.4 The Customer shall ensure that it, its Affiliates and each Authorised User shall at all times comply with:

2.4.1 all Data Protection Laws in connection with the processing of Protected Data, the use of the Services (and each part) and the exercise and performance of its respective rights and obligations under our Agreement, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; and

2.4.2 the terms of our Agreement.

2.5 The Customer warrants, represents and undertakes, that at all times:

2.5.1 all Protected Data (if processed in accordance with our Agreement) shall comply in all respects, including in terms of its collection, storage and processing, with Data Protection Laws;

2.5.2 all Protected Data shall comply with clauses 10.3 and 11.2 of the SaaS Terms;

2.5.3 all necessary fair processing and other information notices have been provided to the Data Subjects of the Protected Data (and all necessary consents from such Data Subjects obtained and at all times maintained) to the extent required by Data Protection Laws in connection with all processing activities in respect of the Protected Data which may be undertaken by the Supplier and its Sub-Processors in accordance with our Agreement;

2.5.4 the Protected Data is accurate and up to date;

2.5.5 it shall establish and maintain adequate security measures to safeguard Protected Data in its possession or control from unauthorised access and maintaining complete and accurate copies of all Protected Data provided to the Supplier (or anyone acting on its behalf) so as to be able to immediately recover and reconstitute such Protected Data in the event of loss, damage or corruption of such Protected Data by the Supplier or any other person;

2.5.6 all instructions given by it to the Supplier in respect of Personal Data shall at all times be in accordance with Data Protection Laws; and

2.5.7 it has undertaken due diligence in relation to the Supplier's processing operations and commitments and it is satisfied (and all times its continues to use the Services remains satisfied) that:

(a) the Supplier's processing operations are suitable for the purposes for which the Customer proposes to use the Services and engage the Supplier to process the Protected Data;

(b) the following technical and organisational measures shall (if the Supplier complies with its obligations) ensure a level of security appropriate to the risk in regards to the Protected Data:

(i) all data sent between a web browser and the Supplier's servers shall be encrypted in transit;

(ii) all personally identifiable pupil data shall remain encrypted at rest in the Supplier's database;

(iii) the Supplier's servers are located in a highly secure ISO27001 certified data centre;

(iv) all of the Supplier's staff have an up-to-date enhanced DBS check;

(v) the Supplier's offices are monitored by CCTV and security patrols;

(vi) the Supplier has protocols in place to ensure that Protected Data is handled appropriately, securely and in a legally compliant manner;

(vii) all data is stored within the United Kingdom;

(viii) save for any data processing undertaken by the Supplier's ISO27001 certified UK based data centre provider, the Supplier does not subcontract any data processing activities;

(ix) all of the Supplier's staff are subject to non-disclosure terms and a duty of confidentiality with respect to information that comes into their possession during the course of employment; and

(c) the Supplier has sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of Data Protection Laws.

3 Instructions and details of processing

3.1 Insofar as the Supplier processes Protected Data on behalf of the Customer, the Supplier:

3.1.1 unless required to do otherwise by Applicable Law, shall (and shall take steps to ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Customer's documented instructions as set out in this paragraph 3.1 and paragraphs 3.3 and 3.4 (including when making a Transfer of Protected Data to any International Recipient), as Updated from time to time (**Processing Instructions**); and

3.1.2 if Applicable Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Customer of any such requirement before processing the Protected Data (unless Applicable Law prohibits such information on important grounds of public interest).

3.2 The Customer shall be responsible for ensuring all Authorised Affiliates' and Authorised User's read and understand the Privacy Notice (as Updated from time to time).

3.3 The Customer acknowledges and agrees that the execution of any computer command to process (including deletion of) any Protected Data made in the use of any of the Subscribed Services by an Authorised User will be a Processing Instruction (other than to the extent such command is not fulfilled due to technical, operational or other reasons). The Customer shall ensure that Authorised Users do not execute any such command unless authorised by the Customer (and by all other relevant Controller(s)) and acknowledge that if any Protected Data is deleted pursuant to any such command the Supplier is under no obligation to seek to restore it.

3.4 Subject to applicable Subscribed Service Specific Terms or the Order Form the processing of the Protected Data by the Supplier under our Agreement shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in the schedule.

4 Technical and organisational measures

4.1 Taking into account the nature of the processing, the Supplier shall implement and maintain, at its cost and expense, the technical and organisational measures:

4.1.1 in relation to the processing of Protected Data by the Supplier, as set out in clause 2.5.7(b); and

4.1.2 to assist the Customer insofar as is possible in the fulfilment of the Customer's obligations to respond to Data Subject Requests relating to Protected Data, in each case at the Customer's cost on a time and materials basis.

5 Using staff and other processors

5.1 The Supplier shall not engage any Sub-Processor for carrying out any processing activities in respect of the Protected Data except in accordance with our Agreement without the Customer's written authorisation of that specific Sub-Processor (such authorisation not to be unreasonably withheld, conditioned or delayed).

5.2 The Customer authorises the appointment of an ISO27001 certified data centre responsible for the provision of dedicated (to the Supplier) secure storage facilities essential to the provision of the Subscribed Services.

5.3 The Supplier shall:

5.3.1 prior to the relevant Sub-Processor carrying out any processing activities in respect of the Protected Data, appoint each Sub-Processor under a written contract containing materially the same obligations as under paragraphs 2 to 12 (inclusive) that is enforceable by the Supplier (including those relating to sufficient guarantees to implement appropriate technical and organisational measures);

5.3.2 ensure each such Sub-Processor complies with all such obligations; and

5.3.3 remain fully liable for all the acts and omissions of each Sub-Processor as if they were its own.

5.4 The Supplier shall ensure that all persons authorised by it (or by any Sub-Processor) to process Protected Data are subject to a binding written contractual obligation to keep the Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case the Supplier shall, where practicable and not prohibited by Applicable Law, notify the Customer of any such requirement before such disclosure).

6 Assistance with compliance and Data Subject rights

6.1 The Supplier shall refer all Data Subject Requests it receives to the Customer without undue delay. The Customer shall pay the Supplier for all work, time, costs and expenses incurred in connection with such activity, calculated at the Supplier's rates set out in the Supplier's Standard Pricing Terms.

6.2 The Supplier shall provide such reasonable assistance as the Customer reasonably requires (taking into account the nature of processing and the information available to the Supplier) to the Customer in ensuring compliance with the Customer's obligations under Data Protection Laws with respect to:

6.2.1 security of processing;

6.2.2 data protection impact assessments (as such term is defined in Data Protection Laws);

6.2.3 prior consultation with a Supervisory Authority regarding high risk processing; and

6.2.4 notifications to the Supervisory Authority and/or communications to Data Subjects by the Customer in response to any Personal Data Breach,

provided the Customer shall pay the Supplier for all work, time, costs and expenses incurred in connection with providing the assistance in this paragraph 6.2, calculated at the Supplier's rates set out in the Supplier's Standard Pricing Terms.

7 International data transfers

7.1 Subject to paragraph 7.2, the Supplier shall not Transfer any Protected Data:

7.1.1 from any country to any other country; and/or

7.1.2 to an organisation and/or its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries,

without the Customer's prior written consent except where the Supplier is required to Transfer the Protected Data by Applicable Law (and shall inform the Customer of that legal requirement before the Transfer, unless those laws prevent it doing so).

7.2 The Customer agrees that the Supplier may Transfer any Protected Data for the purposes referred to in paragraph 3.4 to any International Recipient(s), provided all Transfers by the Supplier of Protected Data to an International Recipient (and any Onward Transfer) shall be (to the extent required under Data Protection Laws) effected by way of Appropriate Safeguards and in accordance with Data Protection Laws and our Agreement. The provisions of our Agreement shall constitute the Customer's instructions with respect to Transfers in accordance with paragraph 3.1.1.

7.3 The Appropriate Safeguards employed by the Supplier in connection with our Agreement shall be as follows:

7.4 The Supplier (or its Sub-Processors) may only process Protected Data in the UK or EEA.

7.5 The Customer acknowledges that due to the nature of internet-based services, the Protected Data may also be Transferred to other geographical locations in connection with use of the Service further to access and/or computerised instructions initiated by Authorised Users. The Customer acknowledges that the Supplier does not control such processing and the Customer shall ensure that Authorised Users (and all others acting on its behalf) only initiate the Transfer of Protected Data to other geographical locations if Appropriate Safeguards are in place and that such Transfer is in compliance with all Applicable Laws.

8 Information and audit

8.1 The Supplier shall maintain, in accordance with Data Protection Laws binding on the Supplier, written records of all categories of processing activities carried out on behalf of the Customer.

8.2 The Supplier shall, on request by the Customer, in accordance with Data Protection Laws, make available to the Customer such information as is reasonably necessary to demonstrate the Supplier's compliance with its obligations under this Data Protection Addendum and Article 28 of the GDPR (and under any Data Protection Laws equivalent to that Article 28), and allow for and contribute to audits, including inspections, by the Customer (or another auditor mandated by the Customer) for this purpose provided:

8.2.1 such audit, inspection or information request is reasonable, limited to information in the Supplier's (or any Sub-Processor's) possession or control and is subject to

the Customer giving the Supplier reasonable prior notice of such audit, inspection or information request;

8.2.2 the parties (each acting reasonably and consent not to be unreasonably withheld or delayed) shall agree the timing, scope and duration of the audit, inspection or information release together with any specific policies or other steps with which the Customer or third party auditor shall comply (including to protect the security and confidentiality of other customers, to ensure the Supplier is not placed in breach of any other arrangement with any other customer and so as to comply with the remainder of this paragraph 8.2);

8.2.3 all costs of such audit or inspection or responding to such information request shall be borne by the Customer, and the Supplier's costs, expenses, work and time incurred in connection with such audit or inspection shall be reimbursed by the Customer on a time and materials basis in accordance with the Supplier's Standard Pricing Terms;

8.2.4 the Customer's rights under this paragraph 8.2 may only be exercised once in any consecutive 12month period, unless otherwise required by a Supervisory Authority or if the Customer (acting reasonably) believes the Supplier is in breach of this Data Protection Addendum;

8.2.5 the Customer shall promptly (and in any event within [*one*] Business Day) report any non-compliance identified by the audit, inspection or release of information to the Supplier;

8.2.6 the Customer shall ensure that all information obtained or generated by the Customer or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure required by Applicable Law);

8.2.7 the Customer shall ensure that any such audit or inspection is undertaken during normal business hours, with minimal disruption to the businesses of the Supplier and each Sub-Processor; and

8.2.8 the Customer shall ensure that each person acting on its behalf in connection with such audit or inspection (including the personnel of any third party auditor) shall not by any act or omission cause or contribute to any damage, destruction, loss or corruption of or to any systems, equipment or data in the control or possession of the Supplier or any Sub-Processor whilst conducting any such audit or inspection.

9 Breach notification

9.1 In respect of any Personal Data Breach involving Protected Data, the Supplier shall, without undue delay (and in any event within 72 hours):

9.1.1 notify the Customer of the Personal Data Breach; and

9.1.2 provide the Customer with details of the Personal Data Breach.

10 Deletion of Protected Data and copies

Following the end of the provision of the Services (or part) relating to the processing of Protected Data the Supplier shall dispose of Protected Data in accordance with its obligations under our Agreement. The Supplier shall have no liability (howsoever arising, including in negligence) for any deletion or destruction of any such Protected Data undertaken in accordance with our Agreement.

11 Compensation and claims

11.1 The Supplier shall be liable for Data Protection Losses (howsoever arising, whether in contract, tort (including negligence) or otherwise) under or in connection with our Agreement:

11.1.1 only to the extent caused by the processing of Protected Data under our Agreement and directly resulting from the Supplier's breach of our Agreement; and

11.1.2 in no circumstances to the extent that any Data Protection Losses (or the circumstances giving rise to them) are contributed to or caused by any breach of our Agreement by the Customer.

11.2 If a party receives a compensation claim from a person relating to processing of Protected Data in connection with our Agreement or the Services, it shall promptly provide the other party with notice and full details of such claim. The party with conduct of the action shall:

11.2.1 make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of the other party (which shall not be unreasonably withheld or delayed); and

11.2.2 consult fully with the other party in relation to any such action but the terms of any settlement or compromise of the claim will be exclusively the decision of the party that is responsible under our Agreement for paying the compensation.

11.3 The parties agree that the Customer shall not be entitled to claim back from the Supplier any part of any compensation paid by the Customer in respect of such damage to the extent that the Customer is liable to indemnify or otherwise compensate the Supplier in accordance with our Agreement.

11.4 This paragraph 11 is intended to apply to the allocation of liability for Data Protection Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

11.4.1 to the extent not permitted by Applicable Law (including Data Protection Laws); and

11.4.2 that it does not affect the liability of either party to any Data Subject.

12 Survival

This Data Protection Addendum (as Updated from time to time) shall survive termination (for any reason) or expiry of our Agreement and continue until no Protected Data remains in the possession or control of the Supplier or any Sub-Processor, except that paragraphs 10 to 12 (inclusive) shall continue indefinitely.

13 Data protection enquiries

Please address any enquiries on data protection matters to dataprotection@speechlink.co.uk

THE SCHEDULE
DATA PROCESSING DETAILS

Subject-matter of processing:

- the performance of respective rights and obligations under our Agreement and delivery and receipt of the Services under our Agreement.

Duration of the processing:

- until the earlier of final termination or final expiry of our Agreement, except as otherwise expressly stated in our Agreement.

Nature and purpose of the processing:

- processing in accordance with the rights and obligations of the parties under our Agreement.
- processing as reasonably required to provide the Services.
- processing as initiated, requested or instructed by Authorised Users in connection with their use of the Services, or by the Customer, in each case in a manner consistent with our Agreement.
- in relation to each Subscribed Service, otherwise in accordance with the nature and purpose identified in its Subscribed Service Specific Terms.

Type of Personal Data:

Authorised Users:

- Email address
- Forename and surname
- Role
- Place of work

Children undergoing speech / language assessments:

- Forename and Surname
- Date of Birth
- SEN status
- English as an Additional Language (EAL)
- Gender
- Pupil Premium or other indicator of social deprivation
- School year
- Form

Some implementations of the Supplier's packages enable Customers to create additional data fields for their own uses.

Categories of Data Subjects:

- Authorised Users
- Children undergoing speech/language assessments

Special categories of Personal Data:

The Supplier does not by default process any specifically special category data.