DATA PROCESSING AGREEMENT

This DPA forms part of the Agreement between the Controller and the Processor. It sets out the terms on which the Processor processes Personal Data on behalf of the Controller in providing the Services. Under clause 10.2 of the Terms, the Processor is a data processor and the Controller is a data controller.

1. Definitions

Any capitalised term not defined in this DPA has the meaning given to it in the Terms.

"Affiliate"	means any entity that directly or indirectly controls, is controlled by, or is under common control of a party. "Control" means direct or indirect ownership or control of more than 50% of the voting interests of a party;
"Agreement"	has the meaning given in the Terms, being the Terms, this DPA and the Privacy Policy together;
"CCPA"	means the California Consumer Privacy Act of 2018, as amended (including by the California Privacy Rights Act) and its regulations;
"Child User"	has the meaning given in the Privacy Policy;
"Controller"	means the Customer (as defined in the Terms), being the school, academy, trust, local authority, district or other educational institution on whose behalf the Services are ordered. Where an individual teacher or employee completes the registration form, they do so on behalf of that institution;
"Data Protection Law"	means all laws and regulations applicable to the processing of Personal Data under the Agreement, including the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003, the EU GDPR and national laws implementing or supplementing it, the FADP and the CCPA, each as amended, replaced or updated from time to time;
"Data Subject"	has the meaning given in Data Protection Law and includes a "Consumer" as defined in the CCPA;
"DPA"	means this data processing agreement, including Exhibits A, B and C;
"EEA"	means the European Economic Area;
"Effective Date"	has the meaning given in the Terms;
"EU GDPR"	means Regulation (EU) 2016/679 (General Data Protection Regulation);

"FADP"	means the Swiss Federal Act on Data Protection of 25 September 2020 and its ordinances;
"Personal Data"	means any personal data (as defined in Data Protection Law) that the Processor processes on behalf of the Controller in providing the Services;
"Personal Data Breach"	has the meaning given in clause 10.1;
"Privacy Policy"	means the Processor's privacy policy published at www.languagenut.com/en-gb/privacy-policy, which describes the Processor's processing as a controller and does not apply to Personal Data processed under this DPA;
"Processor"	means Languagenut Limited, a company registered in England and Wales under number 07401600, including where applicable a "Service Provider" as defined in the CCPA;
"Restricted Transfer"	means (i) where the EU GDPR applies, a transfer of Personal Data from the EEA to a country outside the EEA not subject to an adequacy decision of the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data from the UK to a country not covered by adequacy regulations under section 17A of the Data Protection Act 2018; and (iii) where the FADP applies, a transfer of Personal Data from Switzerland to a country not recognised as adequate by the Swiss Federal Council;
"SCCs"	means (i) the standard contractual clauses annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 ("EU SCCs"); (ii) the EU SCCs as supplemented by the International Data Transfer Addendum issued by the Information Commissioner, as set out in Exhibit C ("UK Addendum"); and (iii) the EU SCCs as adapted under clause 7.4 ("Swiss SCCs");
"Services"	has the meaning given in the Terms, being the Languagenut online language-learning platform and related support;
"Sub-processor"	means any third party (including an Affiliate of the Processor) engaged by the Processor to process Personal Data in providing the Services;
"Sub-processor List"	means the Third Party Supplier List published in the Privacy Policy, as updated under clause 6;
"Supervisory Authority"	means a governmental or government-chartered regulatory body with binding legal authority over a party;
"Terms"	means the Processor's Terms of Service published at www.languagenut.com/en-gb/terms;

"UK GDPR"	means the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended.

2. Purpose

2.1 The Processor provides the Services to the Controller under the Agreement. In doing so, the Processor processes Personal Data on behalf of the Controller and will protect that Personal Data in accordance with this DPA.

3. Scope

3.1 The Processor shall process Personal Data only to the extent necessary to provide the Services, in accordance with the Agreement, this DPA and the Controller's documented instructions, including with regard to Restricted Transfers. The Agreement and the Controller's use and configuration of the Services are the Controller's complete instructions at the Effective Date.

3.2 The Controller and Processor shall each ensure that any person acting under their authority who has access to Personal Data does not process it except on the Controller's instructions, unless required to do so by Data Protection Law.

4. Processor's Obligations

4.1 The Processor shall process Personal Data only within the scope of this DPA and on the documented instructions of the Controller, unless required to do otherwise by law, in which case the Processor shall inform the Controller of that legal requirement before processing unless the law prohibits this.

4.2 The Processor shall promptly inform the Controller if, in its opinion, an instruction from the Controller breaches Data Protection Law.

4.3 The Processor shall ensure that all employees, agents, officers and contractors who handle Personal Data: (i) are bound by a duty of confidentiality; (ii) have received appropriate data protection and security training; and (iii) access Personal Data only as necessary for their role.

4.4 The Processor shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing, and the risk to the rights and freedoms of natural persons, including the risk to children. As a minimum, the Processor shall maintain the measures described in Exhibit B.

4.5 The measures in Exhibit B are subject to development and review. The Processor may replace them with alternative measures, provided the overall level of protection is not reduced.

4.6 The Processor may access Personal Data to respond to technical problems or Controller queries and to ensure the proper working of the Services. All such access shall be limited to those purposes.

4.7 Taking into account the nature of the processing and the information available to it, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as possible, to respond to requests from Data Subjects exercising their rights and to meet the Controller's obligations under Articles 32 to 36 of the UK GDPR (and the EU GDPR where applicable).

4.8 The Processor shall not: (i) sell or share Personal Data (as those terms are defined in the CCPA); (ii) retain, use or disclose Personal Data for any purpose other than providing the Services under the Agreement; (iii) use Personal Data for advertising, marketing or profiling, or send marketing communications to Child Users; or (iv) use Personal Data, or permit any Sub-processor to use Personal Data, to train artificial intelligence or machine-learning models.

4.9 The Processor may create anonymised and aggregated data derived from the use of the Services that does not identify, and cannot reasonably be used to identify, any individual or the Controller, and may use it to

maintain, improve and report on the Services. The Processor shall not attempt to re-identify any individual from such data.

4.10 The Processor shall apply the protections for Child Users described in the Privacy Policy when providing the Services, including age-appropriate content, no marketing communications, avatar only profiles, and no linking of Child User accounts to external services.

4.11 The Controller gives the Processor general written authorisation to engage Sub-processors. The Sub-processors listed on the Privacy Policy on the Effective Date are approved.

4.12 The Processor will have a written contract with each Sub-processor that imposes data protection obligations no less protective than this DPA. Clause 11.2 applies to each Sub-processor.

4.13 The Processor will give the Controller at least 30 days' notice before adding or replacing a Sub-processor. It will do this by updating the list on the Privacy Policy and emailing the contact named in the Controller's account. The notice will name the Sub-processor, its location and the processing it will carry out.

4.14 The Controller may object in writing on reasonable data protection grounds within 30 days of the notice. The parties will then discuss the concern in good faith. The Processor may either not use the new Sub-processor for the Controller's Personal Data, or propose a change to the Services that avoids it.

4.15 If the parties cannot resolve the objection within 30 days, the Controller may end the affected part of the Services by written notice.

4.16 Where a Sub-processor must be replaced urgently for security or service continuity reasons, the Processor may do so straight away. It will give notice as soon as it can, and clauses 4.14 and 4.15 still apply.

5. Controller's Obligations

5.1 The Controller represents and warrants that: (i) it shall comply with this DPA and its obligations under Data Protection Law; (ii) it has a lawful basis for the processing, has given all required notices and, where required, has obtained the agreement of those with parental responsibility for Child Users as described in the Privacy Policy; and (iii) all Affiliates of the Controller that use the Services shall comply with the Controller's obligations under this DPA.

5.2 The Controller shall not submit special category data (including data about health, special educational needs, safeguarding, biometrics, ethnicity or religion) or data about criminal convictions or offences to the Services.

5.3 The Controller shall implement appropriate technical and organisational measures on its side, including keeping user credentials confidential and promptly removing access for users who leave.

5.4 Some instructions from the Controller, including the Processor assisting with audits, inspections, DPIAs or other assistance under this DPA, may result in additional fees. In such case the Processor shall notify the Controller of its fees in advance and may charge its reasonable costs and expenses, unless agreed otherwise in writing.

6. Sub-processors

6.1 The Controller gives general written authorisation for the Processor to engage the Sub-processors named in the Sub-processor List at the Effective Date, and Affiliates of the Processor, to process Personal Data in providing the Services.

6.2 Before any Sub-processor processes Personal Data, the Processor shall: (i) carry out appropriate due diligence on its security and data protection practices; and (ii) appoint it under a written contract containing data protection obligations no less protective than those in this DPA.

6.3 The Processor shall give the Controller at least 30 days' prior notice by email of any intended addition or replacement of a Sub-processor, and shall update the Sub-processor List accordingly.

6.4 In Clause 9 of the EU SCCs Option 2 applies, and Sub-processor changes shall be notified and may be objected to as set out in clauses 4.11 to 4.16 of this DPA6.5 The Processor remains liable to the Controller for the performance of each Sub-processor's obligations in accordance with clause 12.

7. Location of Processing and Restricted Transfers

7.1 Where the Controller is established in the United Kingdom, Personal Data about pupils is hosted and stored in the United Kingdom. Limited Personal Data about the Controller's staff and users (for example name, email address and support enquiries) may be processed outside the United Kingdom by the Sub-processors identified in the Sub-processor List.

7.2 Any Restricted Transfer, whether from the Controller to the Processor or from the Processor to a Sub-processor, shall be made only on the basis of an adequacy decision or regulations, or subject to the applicable SCCs or another safeguard permitted by Data Protection Law.

7.3 The EU SCCs apply to Restricted Transfers from the EEA and are incorporated into this DPA by reference, completed as follows:

(i) Module Two (Controller to Processor) applies where the Controller transfers Personal Data to the Processor;

(ii) Module Three (Processor to Processor) applies where the Processor transfers Personal Data to a Sub-processor;

(iii) in Clause 7, the optional docking clause does not apply;

(iv) in Clause 9, Option 2 applies and the time period for notice of Sub-processor changes is as set out in clause 6.3 of this DPA;

(v) in Clause 11, the optional language does not apply;

(vi) in Clause 13, the competent supervisory authority is as set out in Part C of Exhibit A;

(vii) in Clause 17, Option 1 applies and the EU SCCs are governed by the laws of Ireland;

(viii) in Clause 18(b), disputes shall be resolved by the courts of Ireland;

(ix) Annex I is completed with the information in Exhibit A, and Annex II with the information in Exhibit B.

7.4 Where the FADP applies to a Restricted Transfer, the EU SCCs as completed under clause 7.3 are adapted as follows: (i) the Swiss Federal Data Protection and Information Commissioner ("FDPIC") is the competent supervisory authority for transfers governed by the FADP; (ii) references to the GDPR are to be read as references to the FADP insofar as the transfer is subject to the FADP; and (iii) the term "member state" shall not be interpreted so as to exclude Data Subjects in Switzerland from bringing claims in their place of habitual residence under Clause 18(c).

7.5 The UK Addendum in Exhibit C applies to Restricted Transfers from the United Kingdom and is incorporated into this DPA by reference.

7.6 If any provision of this DPA conflicts with the applicable SCCs, the SCCs prevail.

8. Data Subject Requests

8.1 The Controller may require correction, deletion, restriction or export of Personal Data during the term of the Agreement. The Processor shall action such requests to the extent lawful and in accordance with its standard procedures, and in any event within 30 days.

8.2 If the Processor receives a request from a Data Subject relating to Personal Data, it shall refer the Data Subject to the Controller without undue delay, unless prohibited by law. The Controller shall reimburse the Processor's reasonable costs of assisting with a Data Subject request beyond the functionality of the Services. If the Processor is legally required to respond to a Data Subject directly, the Controller shall cooperate with the Processor.

9. Audit

9.1 The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with this DPA and Article 28 of the UK GDPR, and shall allow for and contribute to audits and inspections.

9.2 An audit shall first consist of review of the Processor's most recent certifications, penetration test summaries and policies. If these are not reasonably sufficient, the Controller may conduct a more extensive audit which shall be: (i) at the Controller's expense; (ii) limited in scope to matters specific to the Controller and agreed in advance; (iii) carried out during the Processor's normal business hours on not less than 4 weeks' notice, unless an identifiable material issue has arisen; and (iv) conducted so as not to disrupt the Processor's business.

9.3 This clause does not limit any audit right of the Controller or a Supervisory Authority under Data Protection Law.

10. Personal Data Breach

10.1 The Processor shall notify the Controller without undue delay, and in any event within 48 hours, after becoming aware of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data ("Personal Data Breach").

10.2 The notification shall, to the extent then known, describe: (i) the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and records concerned; (ii) the likely consequences; (iii) the measures taken or proposed to address it and mitigate its effects; and (iv) the contact details of the Processor's Data Protection Officer. Where information is not available at first, the Processor shall provide it in phases without undue delay.

10.3 The Processor shall take all reasonable measures to contain and remedy the Personal Data Breach and shall assist the Controller in meeting its obligations to notify the relevant Supervisory Authority and affected Data Subjects. Notification of a Personal Data Breach is not an acknowledgement of fault or liability.

11. Compliance, Cooperation and Response

11.1 The Processor shall notify the Controller promptly of any request or complaint about the processing of Personal Data that adversely affects the Controller, unless prohibited by law or court order.

11.2 The Processor may retain copies of Personal Data only where required by law, and shall keep such copies confidential and use them only for the purpose of that legal requirement.

11.3 The Processor shall reasonably assist the Controller with data protection impact assessments and prior consultations with a Supervisory Authority, taking into account the nature of the processing and the information available to the Processor.

11.4 If a change in Data Protection Law requires changes to this DPA or to the measures in Exhibit B, the parties shall cooperate to make them. If the Processor cannot accommodate a necessary change, the Controller may terminate the affected part of the Services. Services not affected shall continue.

11.5 The parties shall cooperate, on request, with a Supervisory Authority in the performance of their obligations under this DPA and Data Protection Law.

12. Liability

12.1 The limitations and exclusions of liability in the Terms apply to all claims arising under or in connection with this DPA, save where Data Protection Law does not permit them to apply.

12.2 The Processor is liable for breaches of this DPA caused by the acts, omissions or negligence of its Sub-processors to the same extent as if they were its own, subject to clause 12.1.

12.3 The Controller is liable for breaches of this DPA caused by its Affiliates as if they were its own.

12.4 Neither party may recover more than once for the same loss.

13. Term and Termination

13.1 This DPA starts on the Effective Date and ends automatically on termination or expiry of the Agreement, save that clauses 11.2, 12 and 14 continue for as long as the Processor holds any Personal Data.

14. Return and Deletion of Personal Data

14.1 The Controller may export or request return of Personal Data at any time during the term. If the Controller requests it in writing within 30 days after termination of the Agreement, the Processor shall return the Personal Data in its then current format (CSV) free of charge. Return in any other format may be charged on a time and materials basis, in line with the Terms.

14.2 The Processor shall permanently delete Personal Data from its live systems within 90 days after termination of the Agreement or deactivation of the Controller's account. Copies held in backups shall be deleted as the backups expire, and in any event within a further 90 days. The Processor shall ensure its Sub-processors do the same.

14.3 The Controller may instruct earlier deletion at any time, and the Processor shall action it within 30 days. On request, the Processor shall confirm deletion in writing.

14.4 Clauses 14.2 and 14.3 do not apply to Personal Data that the Processor is required by law to retain, which shall be governed by clause 11.2.

15. General

15.1 If any provision of this DPA is or becomes invalid, the remaining provisions are unaffected, and the invalid provision shall be replaced by a valid provision that comes closest to the parties' intention.

15.2 In the event of any conflict concerning the processing of Personal Data, the following order of precedence applies: (i) the SCCs; (ii) this DPA; (iii) the Terms. The Privacy Policy does not govern the processing of Personal Data under this DPA.

15.3 The Processor may amend this DPA by giving the Controller 30 days' notice by email, in line with the Terms, provided that no amendment reduces the overall protection of Personal Data.

15.4 Subject to the SCCs, this DPA is governed by the laws of England and Wales and the courts of England have exclusive jurisdiction to settle any dispute arising under it.

Exhibit A

List of Parties, Description of Processing and Transfers, Competent Supervisory Authority

A. LIST OF PARTIES The Controller

Name	The Customer, being the educational institution named in the Agreement.
Address	As set out for the Customer in the Agreement.
Contact person's name, position and contact details	As provided by the Customer in its account and used for notification and invoicing purposes.
Activities relevant to the data transferred	Use of the Services to support language teaching and learning.
Signature and date	By entering into the Agreement, the Controller is deemed to have signed the SCCs incorporated into this DPA, including their Annexes, as of the Effective Date.
Role	Data exporter (where a Restricted Transfer takes place).
Representative (if applicable)	Any UK or EU representative named in the Controller's privacy notice.

The Processor

Name	Languagenut Limited (company number 07401600).
Address	Projects The Lanes, Nile House, Nile Street, Brighton, BN1 1HW, England.
Contact person's name, position and contact details	Cameron Law, Chief Technology Officer and Data Protection Officer, cameron@languagenut.com.
Activities relevant to the data transferred	Provision of the Languagenut online language-learning platform and related customer support to schools and other educational institutions.
Signature and date	By entering into the Agreement, the Processor is deemed to have signed the SCCs incorporated into this DPA, including their Annexes, as of the Effective Date.
Role	Data importer (where a Restricted Transfer takes place).

B. DESCRIPTION OF PROCESSING AND TRANSFERS

Categories of Data Subjects	Pupils and students authorised by the Controller to use the Services, including Child Users. Teachers and other staff of the Controller authorised to use the Services.

	School administrators and other contacts of the Controller who manage the account or contact support.
Categories of Personal Data	**Pupils:** ● first name and surname, username and password, school, class or group, and year group; ● where the Controller uses an MIS integration, the MIS identifier used to keep records in sync; ● learning activity data, such as activities completed, scores, progress, assessment results and time spent; ● avatar choices; ● technical data, such as IP address, approximate location (country or region) derived from IP address, device and browser type, and log-in times. **Staff and administrators:** ● name, email address, school and role, username and password; ● usage and technical data as above; ● the content of support enquiries and feedback.
Special category data	None. The Services do not require, and the Controller shall not submit, special category data (including data about health, special educational needs, safeguarding, biometrics, ethnicity or religion) or data about criminal convictions and offences.
Frequency of processing and transfer	Continuous for the term of the Agreement.
Nature of the processing	Collection, hosting, storage, organisation, retrieval, analysis for reporting to the Controller, support, backup and deletion of Personal Data as necessary to provide the Services.
Purpose of the processing and any transfer	To provide the Services to the Controller, including user accounts, learning content, progress reporting for teachers, and customer support. Personal Data is transferred to Subprocessors only as needed for them to provide their services to the Processor.
Retention period	For the term of the Agreement, then as set out in clause 14 of this DPA (live systems within 90 days of termination, backups within a further 90 days).
Transfers to Sub-processors	The subject matter, nature and duration of processing by each Sub-processor, and its location, are set out in the Sub-processor List (the Third Party Supplier List in the Privacy Policy).

C. COMPETENT SUPERVISORY AUTHORITY

Competent supervisory authority (Clause 13 of the SCCs)	Where the UK GDPR applies: the UK Information Commissioner's Office (ICO). Where the EU GDPR applies: the supervisory authority of the EU Member State in which the Controller is established or, where the
	Controller has appointed a representative under Article 27 EU GDPR, the supervisory authority of the Member State in which that representative is established. Where the FADP applies: the Swiss Federal Data Protection and Information Commissioner (FDPIC).

Exhibit B

Technical and Organisational Security Measures

This Exhibit describes the technical and organisational measures the Processor maintains to protect Personal Data, taking into account the nature, scope, context and purposes of the processing and the risks to the rights and freedoms of natural persons, including children. Where applicable, this Exhibit serves as Annex II to the SCCs.

Hosting and location	The platform and all Personal Data, including pupil data, are hosted on Microsoft Azure servers in the United Kingdom (London). Microsoft Azure data centres are certified to ISO/IEC 27001, 27017 and 27018 and audited to SOC 1, 2 and 3. Amazon Web Services provides cloud hosting services in the United Kingdom, as shown in the Sub-processor List. Pupil Personal Data is not stored outside the United Kingdom. Physical security of the data centres is provided by the hosting providers under their certifications.
Encryption of Personal Data	Personal Data is encrypted at rest using AES-256, including backups. Data in transit between users and the Services, and between internal services, is encrypted using TLS 1.2 or higher. Administrative access to servers is by encrypted SSH keys only; password log-in to servers is disabled.
Confidentiality and access control	Access is granted on a least-privilege, need-to-know basis according to role. Every user has a unique account; shared accounts are not permitted. Staff accounts are approved by the Head of Development and the CEO before creation and are disabled promptly when a person leaves. Access rights are reviewed at least quarterly.
User identification and authentication	Multi-factor authentication is enforced on all administrative and cloud service accounts. Passwords must meet a minimum length of 12 characters or be protected by automatic blocking of common passwords. Log-in to externally accessible services is locked after repeated failed attempts.
Separation of customer data	Each Controller's Personal Data is logically separated so that a school can access only its own users and data. Test and development systems are separated from production.
Network security	Boundary and host firewalls are in place on all servers and devices, including cloud network security groups. Only the ports needed to run the Services are open, and administrative interfaces are restricted to trusted IP addresses.
Secure configuration, patching and malware protection	Systems use supported software only. Unused software and accounts are removed. High-risk and critical security updates are applied within 14 days of release. Company devices run malware protection, and files uploaded to the Services are scanned.
Logging and monitoring	Access to production systems and security events are logged and monitored so that it is possible to review who accessed, entered, changed or deleted Personal Data.

Availability, backup and recovery	Automated daily backups are taken, encrypted, and held with geographic redundancy within the United Kingdom. The Processor maintains a disaster recovery plan and tests restoration of data.
Testing and evaluation	The Processor carries out an independent penetration test at least once a year, together with regular vulnerability scanning, and remediates findings based on risk.
Certification	The Processor maintains UK Cyber Essentials certification, or an equivalent or higher standard, for the term of the Agreement. On written request (no more than once in any 12 months) the Processor shall provide its current certificate and a summary of its latest penetration test, which the Controller shall treat as confidential information.
Personnel and governance	The Processor has appointed a Data Protection Officer. Staff are bound by confidentiality obligations, receive data protection and security training on joining and annually, and are subject to disciplinary action for breach of policy. Information security policies are reviewed at least annually.
Data minimisation	The Services collect only the Personal Data needed to provide them. Pupil email addresses, dates of birth, home addresses and special category data are not required.
Retention and deletion	Personal Data is retained and deleted in accordance with clause 14 of this DPA. Deletion uses secure deletion or cryptographic erasure so that data cannot be recovered.
Data portability	On request, the Processor provides a complete export of the Controller's Personal Data in CSV format within 30 days.
Sub-processors	Sub-processors are subject to due diligence before engagement, are bound by written data protection terms no less protective than this DPA, and are listed in the Sub-processor List. Restricted Transfers are made only in accordance with clause 7.
Incident response	The Processor maintains a documented data breach response plan, led by the CTO and Data Protection Officer, which is tested annually. Controllers are notified in accordance with clause 10.

Exhibit C

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables Table 1: Parties

	Exporter (who sends the Restricted Transfer)	**Importer (who receives the Restricted Transfer)**
Start date	The date set out in Annex I of the Approved EU SCCs.	
Parties' details	Full legal name: the Customer named in the Agreement. Main address: as set out in Annex I of the Approved EU SCCs. Official registration number (if any): where set out in the Agreement.	Full legal name: Languagenut Limited. Main address: Projects The Lanes, Nile House, Nile Street, Brighton, BN1 1HW, England. Official registration number: 07401600.
Key Contact	As set out in Annex I of the Approved EU SCCs.	Cameron Law, Chief Technology Officer and Data Protection Officer, cameron@languagenut.com.
Signature	No signature is required.	No signature is required.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs: the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	**Module in operatio n**	**Clause 7 (Docking Clause)**	**Clause 11 (Option)**	**Clause 9a (Prior Authorisation or General Authorisation)**	**Clause 9a (Time period)**	**Is personal data received from the Importer combined with personal data collected by the Exporter?**
1	No	-	-	-	-	-
2	Yes	Not used	Not used	General Authorisation	30 days	-
3	Yes	Not used	Not used	General Authorisation	30 days	-
4	No	-	-	-	-	No

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in: Annex 1A (List of Parties): Exhibit A, Part A; Annex 1B (Description of Transfer): Exhibit A, Part B; Annex II (Technical and organisational measures): Exhibit B; Annex III (List of Sub-processors): the Subprocessor List.

Table 4: Ending this Addendum when the Approved Addendum Changes

Which Parties may end this Addendum as set out in Section 19: Importer and Exporter.

Part 2: Mandatory Clauses Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides

    greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words: "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection

Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with: "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with: "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with: "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which: (a) makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or (b) reflects changes to UK Data Protection Laws. The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the

Approved Addendum have a substantial, disproportionate and demonstrable increase in: (a) its direct costs of performing its obligations under the Addendum; and/or (b) its risk under the Addendum, and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.