UNIFROG EDUCATION LIMITED

DATA SHARING AGREEMENT

BACKGROUND

(A) Unifrog Education Limited (**Unifrog**) provides students and teachers of the School (as well as certain other School staff) with access to the Unifrog Platform pursuant to the Main Agreement (each as defined below).

(B) To this end, Unifrog and the School need to share with each other certain personal data relating to such students, teachers and staff.

(C) Accordingly, Unifrog and the School now agree to handle such personal data on the terms set out in this Data Sharing Agreement.

AGREED TERMS

1. DEFINITIONS AND INTERPRETATION

1.1 In this Data Sharing Agreement:

Agreed Purposes means for the purposes of the Main Agreement or this Data Sharing Agreement;

"**appropriate technical and organisational measures**", "**controller**", "**data subject**", "**personal data**", "**processing**" and "**processor**" shall have the respective meanings given to them in applicable Data Protection Laws from time to time (and related expressions, including process, processed and processes shall be construed accordingly);

Competent Authority means the UK government, the Information Commissioner's Office or any other competent court or authority in the UK;

Data Protection Laws means:

(a) in the UK: the UK Data Protection Laws;

(b) in the Territory: any laws or regulations of the Territory relating to the protection of personal data;

Data Transfer Impact Assessment means the data transfer impact assessment undertaken by Unifrog at Schedule 3, as shall be amended, revised or replaced from time to time;

Main Agreement means the service terms which can be accessed at https://www.unifrog.org/terms-of-service governing the provision of the Unifrog Platform to the School by Unifrog;

Other School Staff means any staff member of the School (other than a Teacher) who is authorised by Unifrog to access and use the Unifrog Platform;

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

Relevant Personal Data means any personal data which is processed or to be processed by one or both of the parties in connection with the use of the Unifrog Platform, and as further described in clause 4.2;

SCCs means the European Commission's Standard Contractual Clauses for the transfer of personal data from the EEA to controllers established outside the EEA (controller-to-controller transfers) set out in the Annex to Commission Decision 2004/915/EC and adopted by the UK government for transfers of personal data from the UK to controllers established outside the UK, a completed copy of which comprises Schedule 1;

Student means any student or former student of the School who is authorised by Unifrog to access and use the Unifrog Platform;

Supplementary Measures means the provisions of Schedule 2, which set out the supplementary measures to the SCCs to be used in respect of transfers of personal data from Unifrog to the School, to ensure an essentially equivalent level of protection to that which is required under UK Data Protection Laws;

Teacher means any teacher of the School who is authorised by Unifrog to access and use the Unifrog Platform;

Territory means the country where the School is located;

UK GDPR means General Data Protection Regulation ((EU) 2016/679) as incorporated (in whole or in part) into national law in the United Kingdom;

UK Data Protection Laws means the UK GDPR, the Data Protection Act 2018 and any other applicable law or regulation relating to the processing of personal data and to privacy, as such legislation shall be amended, revised or replaced from time to time;

Unifrog Platform means the sections of the Unifrog Website which can only be accessed and used by authorised individuals, including Students, Teachers and Other School Staff;

Unifrog Privacy Policy means the privacy policy specifying the terms on which Unifrog processes Relevant Personal Data, which can be accessed at https://www.unifrog.org/privacy-policy; and

Unifrog Website means the website owned or operated by Unifrog, which can be accessed at www.unifrog.org.

1.2 If there is any conflict or ambiguity between the terms relating to data processing in the Main Agreement and the terms of this Data Sharing Agreement, the terms of this Data Sharing Agreement will prevail.

1.3 Unless otherwise stated, a reference to this Data Sharing Agreement shall include its Schedules.

1.4 If there is a conflict or ambiguity between any provisions in the Main Agreement, the main body of this Data Sharing Agreement and the SCCs, the provisions of the SCCs shall prevail.

2. PURPOSE AND DURATION

2.1 Each party agrees to process Relevant Personal Data only for the Agreed Purposes.

2.2 This Data Sharing Agreement shall come into effect on the date hereof and subject to clause 6.4, shall continue for so long as the parties process Relevant Personal Data for the Agreed Purposes.

3. COMPLIANCE WITH DATA PROTECTION LAWS

3.1 Each party shall comply with all applicable requirements of the Data Protection Laws relating to (i) the processing of any Relevant Personal Data, and/or (ii) the exercise of its rights and obligations under the Main Agreement and this Data Sharing Agreement.

3.2 This Data Sharing Agreement is in addition to, and does not relieve, remove or replace any other obligation set out in the Main Agreement or the Data Protection Laws.

4. DATA PROTECTION OBLIGATIONS

4.1 This clause 4 sets out the framework for the processing of Relevant Personal Data by each party, and defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other and to data subjects.

4.2 The parties acknowledge that they are each data controllers in respect of the Relevant Personal Data, and further acknowledge that the Relevant Personal Data:

(a) relates to data subjects who are Students, Teachers and Other School Staff who access and use the Unifrog Platform (whether before, on or after the date of this Data Sharing Agreement) and, in each case, is further described in the Unifrog Privacy Policy;

(b) as it relates to Students, may include, but is not limited to names; email addresses; postcodes; details of academic performance; details of work experience, educational courses, apprenticeships or training programmes undertaken; interests and hobbies; information contained in (or connected with) survey or questionnaire responses;

(c) as it relates to Teachers, may include, but is not limited to names; email addresses; feedback, opinions and/or comments on Students' academic performance; information contained in (or connected with) survey or questionnaire responses; and

(d) as it relates to Other School Staff, may include, but is not limited to IP addresses and other relevant information obtained from the School.

4.3 Unifrog shall process the Relevant Personal Data for the uses set out in the Unifrog Privacy Policy and as required by applicable law.

4.4 For any Student below the age of 13, the School shall:

(a) ensure that consent to the collection and further processing of the Student's Relevant Personal Data in accordance with the Unifrog Privacy Policy is given or authorised by the holder of parental responsibility over that Student ("**Parental Consent**") before the Student accesses or otherwise uses the Unifrog Platform;

(b) not share any personal data relating to the Student with Unifrog without such Parental Consent; and

(c) promptly notify Unifrog if any Parental Consent is withdrawn.

In each case, Parental Consent shall be given by a statement or a clear affirmative action of the holder of parental responsibility and shall be a freely given, specific, informed and unambiguous indication of their wishes.

4.5 Without prejudice to the generality of clause 3.1, each party shall:

(a) process the Relevant Personal Data fairly and lawfully in accordance with the Data Protection Laws;

(b) take appropriate security and organisational measures to protect against unauthorised or unlawful processing of the Relevant Personal Data and against accidental loss, corruption or destruction of, or damage, to the Relevant Personal Data, appropriate to the harm that might result from such processing or loss, corruption, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and cost of implementing any measures (those measures may include, where appropriate, anonymising, pseudonymising and encrypting the Relevant Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services);

(c) only use processors who have agreed to:

(i) process the Relevant Personal Data in accordance with documented instructions of Unifrog or the School (as applicable); and

(ii) implement appropriate security and organisational measures to safeguard such Relevant Personal Data being processed and have entered into written obligations of confidentiality in respect of such Relevant Personal Data;

(d) ensure that its employees, sub-contractors, agents and consultants who process the Relevant Personal Data have received adequate training on compliance with the data protection obligations set out in this clause 4 and in Data Protection Laws applicable to processing;

(e) not transfer any Relevant Personal Data to a country outside the United Kingdom and the European Economic Area (the "**EEA**") except with the other party's prior written consent, in order to perform its obligations under the Main Agreement;

(f) keep reasonable records of processing activities under its responsibility whether or not required by the Data Protection Laws;

(g) promptly co-operate with the other party in respect of any exercise of rights of a data subject under the Data Protection Laws in respect of that Relevant Personal Data;

(h) promptly notify the other party (and in any event within 48 hours) if it (or any of its employees, sub-contractors, agents or consultants) reasonably suspects or becomes aware of any suspected, actual or threatened occurrence of a Personal Data Breach and provide the other party with such details as it reasonably requires regarding:

(i) the nature of the Personal Data Breach, including, but not limited to, the categories and approximate numbers of data subjects and Relevant Personal Data records concerned;

(ii) any investigations into the Personal Data Breach;

(iii) the likely consequences of the Personal Data Breach; and

(iv) any measures taken, or that it recommends, to address the Personal Data Breach, including to mitigate its possible adverse effects,

provided that, without prejudice to the aforementioned obligations, if it cannot provide all these details within the timeframe specified in this clause 4.5(h), it shall (before the end of such timeframe) provide the other party with reasons for the delay and when it expects to be able to provide the relevant details (which may be phased), and give the other party regular updates on these matters; and

(i) subject to clause 4.8 below promptly (and in any event within four days of receipt) notify the other party if it receives from any data subject whose personal data forms part of the Relevant Personal Data:

(i) any communication seeking to exercise rights conferred on the data subject by the Data Protection Laws (including any withdrawal by a Student or a former Student of consent to use his or her data for any or all purposes); and/or

(ii) any complaint or any claim for compensation arising from or relating to the processing of the Relevant Personal Data.

4.6 Subject to clause 4.7, the School (including its teachers and/or other School staff) may upload or submit to the Unifrog Website Relevant Personal Data relating to any Student or former Student that includes:

(a) data concerning health;

(b) data revealing racial or ethnic origin; and/or

(c) other similar special categories of personal data,

for the purpose of its own internal reporting. Unifrog may use such data in an anonymised aggregated form to help assess the progress of different categories of students (for example different ethnic groups) on a regional or national basis.

4.7 The parties acknowledge their respective obligations under the Data Protection Laws as applicable to the processing of the special categories of personal data set out in clause 4.6, and agree that:

(a) they shall each rely on the condition in article 9(2)(g) of the UK GDPR (substantial public interest, being the equality of opportunity or treatment) or in article 9(2)(j) of the UK GDPR (necessary for statistical purposes in the public interest) as appropriate (and an appropriate lawful basis in article 6 of the UK GDPR) to legitimise such processing;

(b) the School shall throughout the Term maintain in place an appropriate policy document (within the meaning of the DPA 2018) to satisfy the requirements of the DPA 2018 in respect of any processing carried out under article 9(2)(g) of the UK GDPR (equal opportunities); and

(c) they shall each put appropriate safeguards in place as required under article 89(1) of the UK GDPR to protect the rights of the Student or former Student in respect of any processing carried out under article 9(2)(j) of the UK GDPR (statistical purposes), such as minimisation and where appropriate, pseudonymisation or anonymisation.

4.8 If a Student or former Student requests from Unifrog access to his or her Relevant Personal Data, to comply with the UK GDPR Unifrog may (and usually will) disclose all his or her Relevant Personal Data provided by the School. This will include all Relevant Personal Data uploaded or submitted to the Unifrog Website by teachers and/or other School staff. Unifrog will normally try to notify the School if it receives such a request but does not commit to doing so.

4.9 The parties acknowledge their obligations to provide data subjects with the information referred to in articles 13 and 14 of the UK GDPR, and the parties shall each ensure that they have a privacy policy in place which complies with the Data Protection Laws.

5. COMPLIANCE WITH CHAPTER V UK GDPR (PERSONAL DATA ONLY)

5.1 This clause 5 establishes Unifrog's and the School's compliance with Chapter V of the UK GDPR in relation to transfers of Relevant Personal Data.

5.2 Unifrog and the School agree that:

(a) any transfers of Relevant Personal Data to the School shall be governed by the SCCs; and

(b) in respect of all transfers of Relevant Personal Data between them, the SCCs shall apply to the parties as if the parties had separately entered into, fully executed and signed such SCCs, Unifrog being the data exporter and the School being the data importer.

5.3 The parties shall comply with the Supplementary Measures when Unifrog transfers Relevant Personal Data to the School.

5.4 Subject to clause 5.5, if a Competent Authority:

(a) prescribes any new or replacement standard data protection clauses applicable to any transfer of any personal data (including any replacement to the SCCs);

(b) enacts, issues or prescribes any legislation, regulation or case law applicable to such cross-border transfers; or

(c) prescribes any other mechanism, measure or action for the lawful cross-border transfer of such personal data,

the parties shall, as soon as reasonably practicable, execute such new or replacement clauses, amend this Data Sharing Agreement in order to comply with such legislation, regulation or case law, or carry out such mechanism, measure or action (as the case may be).

5.5 If a Competent Authority issues any applicable non-legally binding guidance relevant to this Data Sharing Agreement which the parties believe requires an amendment to this Data Sharing Agreement, the parties shall consult with each other reasonably and in good faith in order to agree an appropriate amendment.

5.6 In addition to Unifrog's right to temporarily suspend the transfer of Relevant Personal Data pursuant to clause VI(a) of Schedule 1, if transfers of the Relevant Personal Data to the School would infringe Schedule 1 or any of the Data Protection Laws or if the Supplementary Measures cannot be taken or prove insufficient, both parties shall consult with each other in order to agree upon a resolution, and Unifrog may suspend transfers of Relevant Personal Data until they can be made lawfully.

5.7 The School acknowledges and accepts the outcome of the Data Transfer Impact Assessment which provides the Supplementary Measures for the transfer of Relevant Personal Data to the School under this Data Sharing Agreement and further agrees to accept any updated or revised measures if the Data Transfer Impact Assessment is amended or updated by Unifrog.

6. GENERAL

6.1 No amendment of this Data Sharing Agreement shall be effective unless it is in writing and signed by or on behalf of each of the parties.

6.2 If any provision of this Data Sharing Agreement is found by any court, tribunal or administrative body of competent jurisdiction to be wholly or partly illegal, invalid, void, voidable or unenforceable it shall, to the extent of such illegality, invalidity, voidness, voidability or unenforceability be deemed severable and the remaining provisions of this Data Sharing Agreement and the remainder of such provision shall, to the fullest extent possible, continue in full force and effect.

6.3 No one other than a party to this Data Sharing Agreement shall have any right to enforce any of its terms.

6.4 If the Main Agreement expires or is terminated for any reason, the provisions of this Data Sharing Agreement which are expressly or by implication intended to survive expiry or termination shall continue in full force and effect after such expiry or termination.

6.5 This Data Sharing Agreement and any dispute or claim arising out of or in connection with it (including any non-contractual claims or disputes) shall be governed by and construed in accordance with the laws of England, and the parties hereby submit to the exclusive jurisdiction of the English courts.

With reference to the Main Agreement: this Data Sharing Agreement is entered into on the date after the Fee is paid which the School decides is the date it wishes to start the annual subscription, or the date at which the Onboarding Process begins - whichever is sooner.

SCHEDULE 1 – STANDARD CONTRACTUAL CLAUSES

For the purposes of the SCCs:

(i) a reference to a provision of Directive 95/46/EC shall be deemed to include equivalent provisions of the UK Data Protection Laws;

(ii) a reference to "the law of the Member State in which the data exporter is established" shall be deemed to mean "the law of the United Kingdom"; and

(iii) a reference to obligations determined by the Member State in which the data exporter is established shall be deemed to refer to an obligation under UK Data Protection Laws.

SET II

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Definitions

For the purposes of the clauses:

a) "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

b) "the data exporter" shall mean the controller who transfers the personal data;

c) "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

d) "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data

exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

h) It will process the personal data, at its option, in accordance with:

   i. the data protection laws of the country in which the data exporter is established, or

   ii. the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data, or

   iii. the data processing principles set forth in Annex A.

   Data importer to indicate which option it selects: **(iii)**

   .....

i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

   i. the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

   ii. the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

   iii. data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

   iv. with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

b) In the event that:

   i. the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

   ii. compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

   iii. the data importer is in substantial or persistent breach of any warranties or

undertakings given by it under these clauses;

iv. a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

v. a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Dated: **the date of this Data Sharing Agreement.**

ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.

8. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

   a) i. such decisions are made by the data importer in entering into or performing a contract with the data subject, and

      ii. the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

   or

   b) where otherwise provided by the law of the data exporter.

ANNEX B

DESCRIPTION OF THE TRANSFER

(To be completed by the parties)

Words and expressions defined in the main body of the Data Sharing Agreement shall have the same meaning in this Annex B to SCCs.

Data subjects
The personal data transferred may concern the following categories of data subjects:

Students, Teachers and Other School Staff whose personal data is stored on the Unifrog Platform.

Purposes of the transfer(s)
The transfer is made for the following purposes:

As set out in the definition of Agreed Purposes in the Data Sharing Agreement.

Categories of data
The personal data transferred concern the following categories of data:

As set out in the definition of Relevant Personal Data in the Data Sharing Agreement.

Recipients
The personal data transferred may be disclosed only to the following recipients or categories of recipients:

- Students, Teachers and Other School Staff.

Sensitive data (if appropriate)
The personal data transferred may concern the following categories of sensitive data:

- data concerning health;
- data revealing racial or ethnic origin;
- data relating to special educational needs; and/or
- other similar special categories of personal data.

Data protection registration information of data exporter

Z357522X

Additional useful information (storage limits and other relevant information)Relevant Personal Data should be:

- stored on secure severs;
- retained for as long as is necessary to fulfil the purposes it is collected for, including for any legal, accounting or reporting obligations.

SCHEDULE 2 – SUPPLEMENTARY MEASURES

The measures listed at sections 5.2 and 5.3 of the Data Transfer Impact Assessment.

SCHEDULE 3 – DATA TRANSFER IMPACT ASSESSMENT

TRANSFER IMPACT ASSESSMENT

REGARDING

DATA PROCESSING AGREEMENT BETWEEN

(1) UNIFROG EDUCATION LIMITED (UNIFROG) AND (2) EACH OF THE NON-EEA SCHOOLS (SCHOOLS)

Review Date: At least annually

Document history:

Version number	Summary of change	Reviewer name and role	Date
1.0	Initial draft	External Legal Counsel of Unifrog - Penningtons Manches Cooper LLP	August 2021

[***WARNING*** *– THE PURPOSE OF THIS DOCUMENT IS TO ASSIST THE PARTIES WITH CARRYING OUT THE DATA TRANSFER ASSESSMENT NOW REQUIRED WHERE STANDARD CONTRACTUAL CLAUSES ARE USED TO LEGITIMISE CROSS-BORDER TRANSFERS; IT DOES NOT GUARANTEE COMPLIANCE WITH APPLICABLE LAWS. THE LAW IN RELATION TO CROSS BORDER TRANSFERS IS EVOLVING AND MUST BE KEPT UNDER CONTINUOUS REVIEW. AS OF THE LAST REVIEW DATE OF THIS DATA TRANSFER IMPACT ASSESSMENT, NO GUIDANCE HAS BEEN ADOPTED BY ANY UK OR EU REGULATOR REGARDING HOW TO CARRY OUT THIS ASSESSMENT, THOUGH THE RECOMMENDATIONS PUBLISHED BY THE EUROPEAN DATA PROTECTION BOARD ARE TAKEN INTO ACCOUNT HERE. AS MORE GUIDANCE IS RELEASED, THE ASSESSMENT SHOULD EVOLVE AND FURTHER STEPS TAKEN AS NECESSARY TO ENSURE COMPLIANCE*.]

1. BACKGROUND

Following the Court of Justice of the European Union's decision in *Schrems II*[1], UK organisations that rely on Standard Contractual Clauses (**SCCs**) to transfer personal data must assess, on a case-by-case, whether the laws of the territory into which personal data is being transferred guarantee data subjects a level of data protection essentially equivalent to that required under UK law. This does not apply to EEA countries or countries which are covered by a UK adequacy regulation.

Transfer accountability framework

The European Data Protection Board (**EDPB**) recommends[2] the following steps in relation to accountability for transfers:

- Step 1: Know your transfers
- Step 2: Identify the transfer tools you are relying upon
- Step 3: Assess whether the transfer tool you are relying upon is effective for all circumstances of the transfer
- Step 4: Adopt supplementary measures if necessary
- Step 5: Procedural steps if supplementary measures are necessary
- Step 6: Re-evaluate at appropriate intervals

The purpose of this document is to provide a framework and means of recording the assessment in relation to the transfer.

Unifrog is based in the UK and delivers an online platform (the "Unifrog Platform") to more than 300 separate Schools located in over 60 territories outside the UK and EEA (as set out in the Schedule), which enables the Schools' students to explore career and apprenticeship opportunities, and post-16 and post-18 option courses. Undertaking a transfer impact assessment in respect of the legal system of each School's territory is unfeasible, especially in light of the resources available to Unifrog, as a relatively small business, and the Schools. In light of the above, Unifrog has decided to carry out one overarching transfer impact assessment in respect of all Schools' jurisdictions, and assess the supplementary measures that can be put in place by the parties to ensure an essentially equivalent level of protection for the relevant personal data once transferred to each destination country.

Unifrog shares the personal data of students with each School to enable students to use the Unifrog Platform. Unifrog also shares data with the Schools so they can invite their students to their alumni programmes and see how their students progress after they have left the School. Unifrog shares the personal data of the School's teachers with the School to enable students to use the Unifrog Platform as intended. The School shares personal data with Unifrog to enable its students,

[1] http://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=EN

[2] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

teachers and other school staff to interact and use the Unifrog Platform as intended. The categories of personal data are set out below.

If Unifrog or any of the Schools determine that the supplementary measures are not effective to bring the level of data protection to that required under UK law, the transfer must be suspended or a different lawful transfer mechanism put in place.

This transfer impact assessment does not guarantee compliance with any applicable laws and must be kept under continuous review, particularly in light of further updated recommendations or guidance that may become available.

2. DATA SHARING AGREEMENT

NOTE: Capitalised words and expressions used below have the same meaning as set out in this Data Sharing Agreement.

2.1	**Contract:** The parties have entered into the Main Agreement, which is supplemented by this Data Sharing Agreement signed by the parties.
2.2	**Need for and purpose of the transfer(s) (step 1 of transfer accountability framework):** The parties need to share with each other personal data of students of the Schools, to enable Unifrog to provide the services described in the Main Agreement.
2.3	**Grounds for transfer (step 2 of transfer accountability framework):** The transfer tool that will be relied upon for the transfer of personal data from Unifrog (in the UK) to the Schools (outside the UK and EEA) is the SCCs. The parties acknowledge that no transfer tool is required for the transfer of personal data from the Schools to Unifrog. This transfer impact assessment therefore only focuses on the transfer of personal data from Unifrog to the Schools.
2.4	**Effectiveness of transfer tool and relevance to all circumstances of the transfer (step 3 of transfer accountability framework):** The SCCs will be relevant to all circumstances of this transfer, and the circumstances of the transfer are further assessed in this transfer impact assessment.
2.5	**Nature of data sharing arrangement:** Controller to controller
2.6	**Name and role of organisation exporting the personal data:** Unifrog (data exporter) – Controller
2.7	**Country/Territory from which personal data is being transferred:** United Kingdom

2.8	**Name and role of organisation importing the personal data:** The School (data importer) - Controller
2.9	**Country/Territory to which personal data is being transferred:** See Appendix
2.10	**Onward transfer of personal data by data importer (if yes, identify to whom the data is transferred and the country of onward transfer):** Students, teachers and other school staff may access the Unifrog Platform (provided that each student may only process his/her/their own data and all access is password-protected). It is not anticipated that any School will transfer the personal data to a recipient outside its own country.

3. DESCRIPTION OF PROCESSING

3.1	**Types of data subject (and separately identify any categories of vulnerable individuals and children whose personal data is being collected or confirm none):** • current and former students of the Schools; • some students are children aged 11-18; • current and former teachers; • current and former school staff.
3.2	**Purpose of the transfer(s):** Provision of the services by Unifrog as set out in the Main Agreement.
3.3	**Categories of data (and identify any categories of special category data being collected or confirm none):** • For current and former students: name; details of education and academic performance; any further education and career opportunities that the student has expressed an interest in; details of any further education or employment undertaken; e-mail address; year of leaving school; information contained in (or connected with) survey or questionnaire responses; • For current and former teachers: email addresses; records of interactions with students; feedback, opinions and/or comments on students' academic performance; information contained in (or connected with) survey or questionnaire responses; and • For current and former school staff: IP addresses and other relevant information obtained from the School. From time to time, the personal data transferred may concern the following categories of special category data: • health records; • racial or ethnic origin

	• data relating to special educational needs.
3.4	**Data minimisation (identify considerations given to data minimisation such as certain types of data subject not included in scope, types of data/fields collected minimised, data flows minimised, de-identification techniques used):** This Data Sharing Agreement requires each party to: *"comply with all applicable requirements of the Data Protection Laws relating to (i) the processing of any Relevant Personal Data, and/or (ii) the exercise of its rights and obligations under the Main Agreement and this Data Sharing Agreement"* (clause 3.1). This Data Sharing Agreement requires the School to: *"process the Relevant Personal Data fairly and lawfully in accordance with the Data Protection Laws"* (clause 4.5(a)). *"they shall each put appropriate safeguards in place as required under article 89(1) of the GDPR to protect the rights of the Student or former Student in respect of any processing carried out under article 9(2)(j) of the GDPR (statistical purposes), such as minimisation and where appropriate, pseudonymisation or anonymisation"* (clause 4.7(c)).
3.5	**Transparency:** The transfers of personal data envisaged by this Data Sharing Agreement are transparently addressed within a privacy notice(s) given to data subjects https://www.unifrog.org/privacy-policy

4. ADEQUACY OF DATA PROTECTION IN DESTINATION COUNTRY

The Court of Justice of the European Union (Court or CJEU) found the SCCs to be valid, but emphasised the obligations they impose. In particular, both parties to the SCCs are required to verify, prior to any transfer, and taking into account the circumstances of the transfer, whether a level of protection essentially equivalent to that guaranteed within the UK by the UK GDPR is respected in the destination country.

EDPB clarifies that "essential equivalence" will not be possible if the data importer is prevented from complying with their obligations under the SCCs (or other Article 46 GDPR transfer tool) due to the destination country's legislation and practices applicable to the transfer.

Relevant factors when making this assessment include (without limitation) the same factors that the European Commission considers when evaluating whether an adequacy decision should be made, as set out in Article 45(2) of GDPR. The

factors set out in Article 45(2) include: the rule of law; respect for human rights and fundamental freedoms; relevant legislation; access by public authorities to personal data; the existence of independent supervisory authorities; effective data subject rights and effective redress for data subjects whose personal data is transferred.

The assessment must consider all actors participating in the transfer (e.g. controllers, processors and sub-processors processing data in the destination country), as identified in the mapping exercise for transfers.

Consideration should also be given to the guarantees set out in the SCCs (i.e. whether the recipient of the data is able to comply with the SCCs in a practical sense) and, as regards access by public authorities to the data transferred, relevant aspects of the destination country's legal system. Where the local laws of the destination country do not provide an essentially equivalent level of protection, supplementary measures to ensure essential equivalence must be implemented, otherwise the transfer cannot take place (see section 5 below).

*The EDPB's recommendations on the European Essential Guarantees for surveillance measures[3] (**EEG Recommendations**) provide additional information on how to assess if access or interception by authorities in the destination country comply with European Standards. The EEG Recommendations refer to CJEU case law and provide that the following criteria (known as the four European Essential Guarantees) should be applied when assessing whether local laws, which limit the data protection and privacy rights recognised by the EU, are justifiable:*

A. *processing should be based on clear, precise and accessible rules;*
B. *necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated;*
C. *an independent oversight mechanism should exist; and*
D. *effective remedies need to be available to the individual.*

The EEG Recommendations comment that: "The four European Essential Guarantees are to be seen as core elements to be found when assessing the level of interference with the fundamental rights to privacy and data protection. They should not be assessed independently, as they are closely interlinked, but on an overall basis, reviewing the relevant legislation in relation to surveillance measures, the minimum level of safeguards for the protection of the rights of the data subjects and the remedies provided under the national law of the third country".

4.1	**Assessment of local laws:** As described in section 1 above, this is an overarching transfer impact assessment in respect of the transfers Unifrog makes to the Schools it works with in numerous non-UK / non-EEA countries around the world.

[3] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en

	It would not be practical to assess the legal framework in each of the countries in which the Schools are located. However, Unifrog considers there is a risk that the laws or practices of those destination countries do not ensure an essentially equivalent level of data protection to that guaranteed under UK / EU law. For instance, in certain destination countries: • applicable laws may impinge on the commitments contained in the SCCs (including commitments enabling data subjects to exercise their rights, such as access, correction and deletion requests for transferred data); • applicable laws may lay down requirements to disclose personal data to public authorities or grant such public authorities powers of access to personal data (for instance for criminal law enforcement, regulatory supervision and national security purposes) that go beyond what is necessary and proportionate in a democratic society; • there may be more limited data protection laws, and/or the data protection authority may not have sufficient independence; or legislation governing the access to data by public authorities may be ambiguous or not publicly available; • data subjects may be unable to obtain redress (as judged against the standards required under UK / EU law). As such, for the purposes of this transfer impact assessement, Unifrog and the Schools shall adopt the same approach in respect of all transfers. Specifically, they shall treat each destination country as though it has a high risk of surveillance measures and does not adhere to the EEG Recommendations, in order to ensure that all transfers are afforded the highest level of protection. Accordingly, additional supplementary measures will need to be adopted in order to improve protection for data which is transferred to all destination countries. Namely, supplementary measures to minimise or eliminate the risk of interception.

5. SUPPLEMENTARY MEASURES

Where the destination country does not provide the level of data protection required by EU and UK law, the parties to the data transfer should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the UK; and whether the law of the destination country will impinge on these supplementary measures so as to prevent their effectiveness.

EDPB recommendations note that:

- *combining diverse measures in a way that support and build on each other may enhance the level of protection and may therefore contribute to reaching EU standards.*

- *contractual and organisational measures alone will generally not overcome access to personal data by public authorities of the destination country (where this unjustifiably interferes with the data importer's obligations to ensure essential equivalence). Indeed, there will be situations where only technical measures might impede or render ineffective access by public authorities in destination countries to personal data, in particular for surveillance purposes. In such situations, contractual or organisational measures may complement technical measures and strengthen the overall level of protection of data, e.g. by creating obstacles for attempts from public authorities to access data in a manner not compliant with EU standards.*

5.1	**Supplementary Measures** **Technical measures** For this transfer the following technical measures will be implemented to supplement the safeguards set out in the SCCs: **Data minimisation** • Unifrog will only send personal data to each School that has been uploaded to the Unifrog Platform by that School's students, teachers and other school staff, except occasionally statistical analysis based on such data. **Encryption** • All data transferred between Unifrog to the School is transmitted using strong encryption – 256-bit SSL/TLS.1.2 (or higher). • Sensitive data such as passwords are hashed and salted. • The Unifrog Platform uses a strong Content Security Policy to help prevent Cross-Site Scripting (XSS), clickjacking and other attacks resulting from code injection. **Other Security** • Only Unifrog's lead developers and Managing Director have access to the servers and technology infrastructures, which are provided by Amazon Web Servers. Servers are automatically updated as soon as security patches are released. • Servers sit behind multiple firewalls within a VPC which is only accessible via a VPN; only ports 80 and 443 are publicly accessible. The database server is not accessible outside the VPC. • Student data and backups are only stored and processed in EU and UK data centres. • Vulnerability assessments are performed regularly, both manually and automatically by the Uniform Platform's developers. Realtime protection is provided by Amazon Web Services and the Unifrog Platform has been externally Penetration Tested.

5.2	**<u>Contractual measures</u>** For the transfer, the following additional contractual measures will be provided to address the risk of interception: • A contractual assurance that all data transferred from Unifrog to the School will be encrypted with 256-bit SSL/TLS.1.2 (or higher) and reliably managed. • A warranty that, to date, the School has not received any orders or other requests from any public authority or law enforcement agency in relation to the data transferred. • A contractual commitment from the School that if it receives any request or order to disclose data received from Unifrog (or any encryption key), it will promptly notify Unifrog, reviewing the legality of any such order, and resist such request or challenge any such order to the extent permitted under applicable law. When challenging such an order, the School shall seek interim measures to suspend the effects of the order until the court has decided on the merits. The School commits not to disclose the personal data requested unless and until a court of competent jurisdiction has ordered it to do so (in which case the School shall, before complying with such order, to the extent permitted by law, give Unifrog as much notice as possible and consult and cooperate with Unifrog regarding appealing such order). If the School is unable to notify Unifrog before complying with any such order, the School shall, in any event, comply with its obligations under SCC Clause II(c) and inform Unifrog (without giving specific details) that it is no longer able to comply with all of the guarantees provided for under the SCCs, so that the transfer of data can be suspended. The School shall also commit to providing the minimum amount of information permissible when responding to the order, based on a reasonable interpretation of the order. The School shall, to the extent permitted by law, document and demonstrate Unifrog the actions it has taken, exercising its best efforts to fulfil the contractual commitments set out in this bullet point. • A contractual commitment from the School to implement the organisational measures set out below.

5.3	**<u>Organisational measures</u>** Unifrog will require the Schools to implement the following organisational measures to complement the technical and contractual measures set out above, in order to ensure an essentially equivalent level of protection of the personal data to that guaranteed within the UK: • the adoption of internal policies with clear allocation of responsibilities for data transfers, and standard operating procedures for cases of official requests from public authorities to access the data. • specific training procedures for School personnel in charge of managing requests for access to personal data from public authorities. • the documentation and recordal of requests for access received from public authorities provided, alongside the reasoning and the actors involved (e.g. whether Unifrog has been notified and its reply, the School's assessment of such requests, *etc*). To the extent permitted by law, these records shall be made available to Unifrog, who should in turn provide them to the data subjects concerned where required. • the adoption of data access and confidentiality policies and best practices, including emphasising the need to keep passwords confidential, and deterring teachers and other school staff from downloading personal data from the Unifrog Platform. • the regular review of internal policies to assess the suitability of the measures referred to above and implement additional or alternative solutions when necessary, to ensure that an equivalent level of protection to that guaranteed within the UK of the personal data transferred is maintained.

6. PROCEDURAL STEPS (STEP 5 OF TRANSFER ACCOUNTABILITY FRAMEWORK)

The EDPB recommendations note that: • If *the selected transfer tool is the SCCs, there is no need to request an authorisation from the competent supervisory authority to add these kind of clauses or additional safeguards as long as the identified supplementary measures do not contradict, directly or indirectly, the SCCs and are sufficient to ensure that the level of protection guaranteed by the GDPR is not undermined. However, the data exporter and importer need to ensure and be able to demonstrate that additional clauses cannot be construed in any way to restrict the rights and obligations in the SCCs or in any other way to lower the level of data protection.*	
6.1	The supplementary measures set out above do not contradict the SCCs relied upon for this transfer. In any event, clause 1.4 of this Data Sharing Agreement addresses this by providing that the SCCs take priority in the event of any conflict or ambiguity. No further procedural steps are needed.

7. ACTIONS

Action required	Owner	Date to be completed
This Data Sharing Agreement will incorporate the supplementary measures set out in sections 5.2 and 5.3	Unifrog and the School	the date that the School confirms its agreement to this Data Sharing Agreement.

8. DECISION

Decision:
Implement the combined supplementary measures identified in section 5 above and proceed with the data transfer, noting that the transfer must be kept under continuous review.

Further guidance from data protection authorities as well as new UK SCCs are anticipated and therefore (a) the transfer tool of the SCCs will need to be updated as and when the new SCCs are finalised and (b) it is also possible that further supplementary measures may be required in the future.

Rationale: implementing the combined supplementary measures identified in section 5 above (comprising technical measures and contractual measures, complemented by the organisational measures) will bring the level of data protection to that required under UK law for the reasons set out in section 5 above.

APPENDIX

SCHOOLS' TERRITORIES OUTSIDE THE EEA (AND NOT COVERED BY AN ADEQUACY DECISION) AS AT JULY 2021

Territory
Albania
Australia
Bahamas
Bahrain
Bermuda
Bermuda
Botswana
Brazil
British Virgin Islands
Brunei Darussalam
Burkina Faso
Cambodia
Cayman Islands
China
Colombia
Costa Rica
Egypt
Fiji
Ghana
Hong Kong
India
Indonesia
Japan
Jordan
Kazakhstan
Kenya
Kosovo
Kuwait
Kyrgyzstan
Lebanon
Macau
Malaysia
Mexico
Monaco
Morocco
Mozambique
Nepal
Nicaragua

Nigeria
Oman
Palestine, State of
Panama
Peru
Philippines
Qatar
Russia
Saudi Arabia
Seychelles
Singapore
Somalia
South Africa
South Korea
Thailand
Ukraine
United Arab Emirates
United States
Uzbekistan
Vietnam
Zambia
Zimbabwe