DATA PROCESSING AGREEMENT

BETWEEN:

(1) **You or your organization or entity** as **the Data Controller** (the “Partner” or the “Data Controller”); and

(2) **Moodle Pty Ltd** being a company registered under the laws of Western Australia with ABN 55 116 513 636 (the “Data Processor").

BACKGROUND

A. This Agreement is to ensure the protection and security of data passed from the Partner to the Data Processor for processing or accessed by the Data Processor on the authority of the Partner for processing or otherwise received by the Data Processor for processing on behalf of the Partner.

B. The Data Processor provides to the Data Controller the Services described in Schedule 1.

C. The provision of such Services involves the processing of Personal Data by the Data Processor on behalf of the Data Controller.

D. The GDPR and the Data Protection Acts place certain obligations upon a Data Controller to ensure that any data processor it engages provides sufficient guarantees to ensure that the processing of the data carried out on its behalf is secure.

E. This Agreement ensures sufficient security guarantees are in place and that any data processing complies with obligations equivalent to those of the GDPR and Data Protection Acts.

F. The terms of this Agreement are to apply to all processing of Personal Data carried out by the Data Processor and to all Personal Data held by the Data Processor on behalf of the Data Controller.

IT IS AGREED

1. DEFINITIONS AND INTERPRETATION

1.1 In this agreement:

“the Data Protection Acts” or "the Acts" means the Data Protection Acts 1988 and 2003 and the Data Protection Act 2018 (when enacted) and EU Directive 95/46/EC;

"Data" means any information of whatever nature that, by whatever means, is provided to the Data Processor by the Partner, is accessed by the Data Processor on the authority of the Partner, or is otherwise received by the Data

Processor on behalf of the Partner, for the purposes of the Processing specified in clause 3.1(a), and shall include, without limitation, any Personal Data;

"Data Subject", "Personal Data" and "Processing" shall have the same meanings as are assigned to those terms in the Acts;

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

“Schedule” means the schedule annexed to and forming part of this Agreement;

"Services" means processing of the Data by the Data Processor in connection with and for the purposes of the provision of the services to be provided by the Data Processor to the Partner under the Services Agreement;

“Services Agreement” means the agreement for the provision of services between the Partner and the Data Processor identified in the Schedule 1.

“Security Measures” means the security measures set out in Schedule 2.

1.2 In this agreement any reference, express or implied, to any enactment (which includes any legislation in any jurisdiction) includes references to:

(a) that enactment as re-enacted, amended, extended or applied by or under any other enactment (before, on or after the date of this agreement);

(b) any enactment which that enactment re-enacts (with or without modification); and

(c) any subordinate legislation made (before, on or after the date of this agreement) under that enactment, as re-enacted, amended, extended or applied as described in clause 1.2(a), or under any enactment referred to in clause 1.2(b).

1.3 In this agreement:

(a) references to a person include an individual, a body corporate and an unincorporated association of persons;

(b) references to a party to this agreement include references to the successors or assignees (immediate or otherwise) of that party.

2. APPLICATION OF THIS AGREEMENT

2.1 The terms of this Agreement apply to all processing of Personal Data carried out for the Data Controller by the Data Processor and to all Personal Data held by the Data Processor in relation to all such processing whether such Personal Data is held at the date of this Agreement or received thereafter. the terms of this Agreement supersede any other arrangement, understanding or agreement

including any services agreement made between the parties at any time relating to protection of Personal Data.

3. DATA PROCESSING

3.1 The Partner acknowledges that it is deemed the Data Controller and Moodle Pty Ltd is deemed the Data Processor at all times and in respect of any personal data processed in the course of providing the Services.

3.2 The Data Processor acknowledges that it is the Data Processor in respect of any personal data that the Partner allows access to or provides to it for the purposes of providing Services to the Partner and that, in such a context, the Partner is the Data Controller.

3.3 The Data Processor takes sole responsibility for its compliance, as data processor, with the requirements of the GDPR and the Data Protection Acts and of the contract herein.

3.4 If the Data Processor processes personal data other than as instructed by the Partner, the Data Processor shall be considered to be a controller in respect of that processing and shall be subject to the rules and legal obligations on data controllers pursuant to the Acts.

3.5 In consideration of the undertakings provided by the Partner in clause 5 of this Agreement, the Data Processor agrees to Process the Data in accordance with this Agreement, and specifically the Data Processor agrees to:

a. process the Data at all times in accordance with the GDPR and the Data Protection Acts and solely for the purposes (connected with provision by the Data Processor of the Services), to the extent and in such manner as is necessary for those purposes and in the manner specified from time to time by the Partner in writing and for no other purpose or in any manner except with the express prior written consent of the Partner;
b. in a manner consistent with the GDPR and the Data Protection Acts and with any guidance issued by the relevant Data protection authority, implement appropriate technical and organizational measures to safeguard the Personal Data from unauthorized or unlawful Processing or accidental loss, destruction or damage*,* and that having regard to the state of technological development and the cost of implementing any measures, such measures shall ensure a level of security appropriate to the harm that might result from unauthorized or unlawful processing or accidental loss, destruction or damage and to the nature of the Data to be protected. the details of those security measures for the time being are set out in Schedule 2 hereto;
c. in particular, ensure that appropriate security measures shall be taken against unauthorized access to, or unauthorized alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. the details of those security measures for the time being are set out in Schedule 2 hereto;

d. comply, in processing of the data, with the Partner's information security policies and procedures as defined or as may be communicated from time to time or specified in the context of a particular project or instance of processing;
e. ensure that each of its employees, agents and subcontractors are made aware of its obligations under this agreement with regard to the security and protection of the Data and shall require that they enter into and enforce binding obligations with the Data Processor in order to maintain the levels of security and protection provided for in this agreement, including the agreement Appended at Schedule 2;
f. not divulge the Data whether directly or indirectly to any person, firm or company or otherwise without the express prior written consent of the Partner except to those of its employees, who are engaged in the Processing of the Data and are subject to written terms substantially the same as the terms contained in this processor agreement or except as may be required by any law or regulation;
g. not divulge the Data, whether directly or indirectly to any person, firm or company or otherwise except with the express prior written consent of the Partner, and to agents or subcontractors who are subject to written terms substantially the same as the terms contained in this processor agreement, or except as may be required by any law or regulation;
h. provide the Partner on demand with the text of any such written terms to which its employees, sub-contractor or agents are subject with regard to their processing of Data;
i. upon the request of the Partner, promptly provide a written description of the technical and organizational measures employed by it and/or any of its permitted sub-contractors, detailed to such a level that the Partner can determine whether or not, in connection with personal data, the Supplier and its permitted subcontractors are complying with their obligations under this Agreement. If, as a result of an independent audit by the Partner, its Agents, or the Office of the Data Protection Commissioner, the measures employed by the Data Processor and/or its permitted subcontractors are not sufficient to ensure compliance with their obligations under this Agreement, the Data Processor shall take all steps (or procure that its permitted sub-contractors take all steps) which are reasonably required to ensure that such compliance is achieved;
j. afford to the Partner (and procure that its permitted sub-contractors afford to the Partner) access on at least 14 working days notice, and at reasonable intervals, to any premises where the relevant personal data are being processed to enable the Partner to ensure that the Data Processor is complying with its obligations under this Agreement and/or that the Data Processor's permitted subcontractors are complying with the equivalent contractual obligations imposed on them;
k. notify the Data Controller (within 2 working days) if it receives:

   i. a request from a data subject to have access to that person's Personal Data

ii. or a complaint or request relating to the Data Controller obligations' under the Act;

l. provide the Data Controller with full cooperation and assistance in relation to any complaint or request made, including by:

i. providing the Data Controller with full details of the complaint or request

ii. complying with a data access request within the relevant timescale set out in the Act and in accordance with the Data Controller's instructions; providing the Data Controller with any Personal Data it holds in relation to a data subject (within the timescales required by the Data Controller)

iii. providing the Data Controller with any information requested by the Data Controller;

m. notify the Data Controller immediately if it becomes aware of:

i. any unauthorized or unlawful processing, loss of, damage to or destruction of any of the Personal Data

ii. or any advance in technology and methods of working which mean that the Data Controller should revise the security measures set out in Schedule 2;

n. in the event of the exercise by Data Subjects of any of their rights under the Acts in relation to the Data directly to the Data Processor, inform the Partner as soon as possible, and the Data Processor further agrees to assist the Partner with all data subject information requests which may be received from any Data Subject in relation to any Data;

o. in the event that the Data Processor receives a request for any information contained in the Data pursuant to the acts, not to respond to the person making such request but to notify the Partner within 2 working days, and the Data Processor further agrees to assist the Partner with all such requests for information which may be received from any person within such reasonable timescales as may be prescribed by the Partner;

p. for the purposes of this Agreement, procure a right in favour of the Partner to enforce the obligations imposed on the Data Processor's permitted subcontractors directly against such sub-contractors and shall also procure that the terms of any sub-contract shall be governed by the Laws of Ireland and be subject to the jurisdiction of the Irish courts;

q. not Process or transfer the Data outside of the European Economic Area except for limited specified purpose and with the express consent of the Partner;

r. to notify all incidents of loss of control of personal data in manual or electronic form to the Partner, as soon as it becomes aware of the incident, such that the Partner can notify the Data Protection Commissioner within 24 hours;

s. in the event of any such breach, to take prompt action to remedy the cause of the breach and to share the costs of such remedy with the Data Controller equally;

t. in the event of any such breach, to share the costs of investigation into said breach with the Data Controller equally;

u. in the event of any such breach, to promptly, and at its own expense provide the Partner on request with all information required to fulfil its obligations, as Data Controller, under all applicable laws, regulations and codes of practice;

v. to otherwise comply with all applicable laws and regulations and with the Personal Data Security Breach Code of Practice insofar as they apply to it;

z. the Data Processor shall maintain the Personal Data processed by the Data Processor on behalf of the Data Controller in confidence, and in particular, unless the Data Controller has given written consent for the Data Processor to do so, the Data Processor shall not disclose any Personal Data supplied to the Data Processor by, for, or on behalf of, the Data Controller to any third party. the Data Processor shall not process or make any use of any Personal Data supplied to it by the Data Controller otherwise than in connection with the provision of the Services to the Data Controller. the above obligations in this Clause 3.5 (z) shall continue for a period of five (5) years after the cessation of the provision of Services by the Data Processor to the Data Controller. Nothing in this Agreement shall prevent either party from complying with any legal obligation imposed by the Data Protection Commissioner or a court. Both parties shall however, where possible, discuss together the appropriate response to any request from the Data Protection Commissioner or court for disclosure of information;

aa. the Data Processor shall take appropriate measures to ensure that the people processing the data on its behalf are subject to a duty of confidence;

bb. the Data Processor shall not subcontract to any third party any of its rights or obligations under this Agreement without the prior written consent of the Data Controller. Where the Data Processor, with the written consent of the Data Controller, does subcontract, it shall do so only by way of a written sub-processing agreement with the subcontractor which imposes the same obligations on the subcontractor as are imposed on the Data Processor under this Agreement and which permits both the Data Processor and the Data Controller to enforce

those obligations. For the avoidance of doubt, where the subcontractor does not meet its obligations under any sub-processing agreement, the Data Processor shall remain fully liable to the Data Controller for meeting its obligations under this Agreement;

cc. the Data Processor shall delete or return all personal data to the Partner, as requested, on the termination of this contract;

dd. the Data Processor shall submit to audits and inspections by or on behalf of the Partner, provide the Partner with whatever information it needs to ensure that they are both meeting their obligations under Article 28 of the GDPR, and will tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state;

ee. This Agreement shall continue in full force and effect for so long as the Data Processor is processing Personal Data on behalf of the Data Controller, and thereafter as provided in Clause 3.5 (z).

4. OBLIGATIONS OF THE PARTNER

4.1 In consideration of the obligations undertaken by the Data Processor in clause 4, the Partner agrees that it shall ensure that it complies at all times with any applicable enactment, and in particular with its obligations as Data Controller under the GDPR and Data Protection Acts.

4.2 In particular, the Partner shall ensure that any disclosure of Personal Data made by it to the Data Processor is made with the data subject's consent, which consent shall have been obtained freely, fairly and after the data subject has been fully informed as to all processing to be applied or is otherwise lawful.

4.3 The Partner shall comply with its responsibilities under all applicable laws, regulations and codes of practice.

5. LIABILITY

5.1 Each party to this Data Processing Agreement commits to being responsible for its own acts of infringement of this Data Processing Agreement. A party shall not be liable for any claims, demands, actions, costs, expenses and liabilities, including reasonable legal fees resulting from the culpable infringement committed by the other party or its current and former trustees, directors, officers, employees, agents, and affiliates. Art. 82 of GDPR is in no way altered by this clause 5.1.

6. TERMINATION

6.1 This agreement shall terminate automatically upon termination or expiry of the Data Processor obligations' in relation to the Services, and on termination of this agreement the Data Processor shall forthwith deliver to the Partner or destroy, at the Partner's sole option, all Data in its possession or under its

control which has been provided by Direct. Either party may terminate this contract on 30 days written notice to the other party, or without notice in the event of a breach of any of the terms of this agreement.

7. WAIVER

7.1 Failure by either party to exercise or enforce any rights available to that party or the giving of any forbearance, delay or indulgence shall not be construed as a waiver of that party's rights under this agreement.

8. INVALIDITY

8.1 If any term or provision of this agreement shall be held to be illegal or unenforceable in whole or in part under any enactment or rule of law such term or provision or part shall to that extent be deemed not to form part of this agreement but the enforceability of the remainder of this agreement shall not be affected provided however that if any term or provision or part of this agreement is severed as illegal or unenforceable, the parties shall seek to agree to modify this agreement to the extent necessary to render it lawful and enforceable and as nearly as possible to reflect the intentions of the parties embodied in this agreement including without limitation the illegal or unenforceable term or provision or part.

9. ENTIRE AGREEMENT

9.1 This agreement and the documents attached to or referred to in this agreement shall constitute the entire understanding between the parties and shall supersede all prior agreements, negotiations and discussions between the parties. In particular the parties warrant and represent to each other that in entering into this agreement they have not relied upon any statement of fact or opinion made by the other, its officers, servants or agents which has not been included expressly in this agreement. Further, each party hereby irrevocably and unconditionally waives any right it may have:

(a) to rescind this agreement by virtue of any misrepresentation;
(b) to claim damages for any misrepresentation whether or not contained in this agreement;

save in each case where such misrepresentation or warranty was made fraudulently.

10. NOTICES

10.1 Notices shall be in writing and shall be sent to the other party marked for the attention of the person at the address set out below. Notices may be sent by mail, email or facsimile transmission. Correctly-addressed notices sent by mail shall be deemed to have been delivered 72 hours after posting and correctly directed email or facsimile transmissions shall be deemed to have been

delivered instantaneously on transmission providing that they are confirmed as set out as above.

If for the Partner: ***email address*** provided to the Data Processor

If for the Data Processor: ***privacy@moodle.com***;

SCHEDULE 1

THE SERVICES AGREEMENT

Description of all Personal Data accepted from the Data Controller:

1) Data Controller's end users/clients personal data processed to set up their profile

   The Data Controller instructs Moodle Pty Ltd to process any and all personal data relating to themselves or to their end users/clients which is uploaded into the hosted learning platform. The Controller warrants that they have received any necessary consents from end users/clients or third parties, if applicable. The personal data required include, but is not limited to, the following fields:

   - First name
   - Surname
   - Email address
   - Country (as applicable)
   - Time zone (as applicable)
   - City/Town (as applicable)
   - End user Picture/Avatar (as applicable)
   - Photographs uploaded by end users/clients (as applicable)
   - any additional personal data uploaded by end users/clients (as applicable)

2) All the activities and functions processed on the website (as Data Controller)

   The hosted learning platform is intended to allow data controllers to specify the nature of data processed, according to their own usage needs. Depending on the choices and setting selected by the Data Controller, these activities may include, but may not be limited to, the upload and storage of documents containing personal data, participation in forum discussions, which will require personal data to be collected and stored on the participants, the collection and processing on usage data, participation in examinations or assessment procedures and video webinars as applicable (including personal data of the participants and observers of the webinar).
   Moodle Pty Ltd uses or might introduce in the future a number of third party organisations to provide certain functionality which allow for the features of the hosted learning platform and user experiences. It is important that the Data Controller notifies their end users/clients of these third party processors, in order to ensure that they have obtained full and informed consent to the data processing involved in the hosted learning platform.

   Moodle Pty Ltd uses:

- Amazon Web Services as a hosting provider. Amazon acts as a subprocessor for Moodle in respect of all data uploaded to the service provided by Moodle.

During the duration of this Agreement Moodle Pty Ltd reserves the right to introduce Google Analytics.

- Google Analytics is used to measure page views on all the websites and solely for statistical purposes. This data can include a user's IP address, geographical location and browser information.

From time to time Moodle Pty Ltd will communicate to the Partner any additional introduction of third party organization as applicable.

Its purpose:

The purpose for this data processing is to provision a functional website, this allows the website' end users/clients to login and use a hosted learning management system.The purpose of the Google Analytics and IntelliBoard data processing is to provide aggregated analysis of how the service is used and its performance.

The processing the Data Controller requires to be performed upon it:

The Data controller requires The Data Processor to process the data provided within the applicable website in the normal operation of a website and to include any of the features specified in the relevant Terms of Service agreed by the Data Controller for the provision of the service.

The hosted learning platform is intended to allow data controllers to specify the nature of data processed, according to their own usage needs. Depending on the choices and setting selected by the Data Controller, these activities may include, but may not be limited to, the upload and storage of documents containing personal data, participation in forum discussions, which will require personal data to be collected and stored on the participants, the collection and processing on usage data, participation in examinations or assessment procedures and video webinars (including personal data of the participants and observers of the webinar as applicable).

SCHEDULE 2

The following are the Security Measures referred to in Sub-Clause 1.1.:

1. The Data Processor will ensure that in respect of all Personal Data it receives from or processes on behalf of the Data Controller it maintains security measures to a standard appropriate to:

1.1 the harm that might result from unlawful or unauthorized processing or accidental loss, damage or destruction of the Personal Data; and

1.2 the nature of the Personal Data.

2. In particular the Data Processor shall:

2.1 ensure that

2.1.1 defines security needs based on a risk assessment;
2.1.2 allocates responsibility for implementing the policy to a specific individual or members of a team;
2.1.3 the required information is disseminated to all relevant staff; and
2.1.4 provides a mechanism for feedback and review.

2.2 ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice;

2.3 prevent unauthorized access to the Personal Data;

2.4 ensure the storage of Personal Data conforms with best industry practice such that the media on which Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled;

2.5 have secure methods in place for the transfer of Personal Data whether in physical form (for instance, by using couriers rather than post) or electronic form (for instance, by using encryption);

2.6 put password protection on computer systems on which Personal Data is stored and ensure that only authorized personnel are given details of the password;

2.7 take reasonable steps to ensure the reliability of employees or other individuals who have access to the Personal Data;
2.8 ensure that any employees or other individuals required to access the Personal Data are informed of the confidential nature of the

Personal Data and comply with the obligations set out in this Agreement;

2.9 ensure that none of the employees or other individuals who have access to the Personal Data publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Data Controller;

2.10 have in place methods for detecting and dealing with breaches of security (including loss, damage or destruction of Personal Data) including:

2.10.1 the ability to identify which individuals have worked with specific Personal Data;
2.10.2 having a proper procedure in place for investigating and remedying breaches of the data protection principles contained in the Acts; and
2.10.3 notifying the Data Controller as soon as any such security breach occurs.

2.11 have a secure procedure for backing up and storing back-ups separately from originals;

2.12 have a secure method of disposal of unwanted Personal Data including for back-ups, disks, print outs and redundant equipment.