DATA SHARING AGREEMENT

THIS DATA SHARING AGREEMENT and its Schedules is incorporated into and forms part of the Subscription Terms between Up Learn and the Customer (as defined in the Subscription Terms).

BACKGROUND

(A) The Customer has agreed to enter into an agreement with Up Learn for the access to online learning courses, on Up Learn's platform.

(B) As part of this agreement, the Customer will need to transfer some limited student and parent data to help facilitate the relationship between the Customer and Up Learn and for the Customer to use Up Learn's online platform.

(C) This Data Sharing Agreement is in place between the parties to ensure that students and parents' personal data is protected and that both the Customer and Up Learn comply with Data Protection Legislation.

AGREED TERMS

1. DEFINITIONS AND INTERPRETATIONS

1.1. The following definitions and rules of interpretation in this clause apply in this Agreement:

Agreed Purposes: To allow students to connect to Up Learn's online platform and receive learning courses (which may include and is not limited to: students creating an account with Up Learn, students using Up Learn's online platform, Up Learn sharing student's results and performance with the student's parent(s) and the student's school); and for the improvement of Up Learn's online platform which may include and is not limited to improvements that benefit the Customer.

Controller, Data Subject, Personal Data, Personal Data Breach, Processing/Process/Processed and Supervisory Authority: are as defined in the UK GDPR.

Effective Date: means the date Effective Date of the Subscription Terms.

Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time in the UK including Regulation (EU) 2016/679 (the "**GDPR**") as defined in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018 ("**UK GDPR**") and the Data Protection Act 2018.

Data Transfer Provisions: means, together, the standard contractual clauses for the transfer of Personal Data to third countries pursuant to the GDPR, adopted by the European Commission under Commission Decision (EU) 2021/914 2021 ("**EU SCCs**") and the UK International Transfer Addendum to the EU SCCs ("**UK Addendum**").

Permitted Recipients: Parents, schools, charities, universities.

Shared Personal Data: the Personal Data to be shared between the parties under clause 4.2. Shared Personal Data shall include, but is not limited to the following categories of information:

- Name;
- Contact Details;
- Age;
- Academic records (including but not limited to school year, results, subjects taken)
- School;

- Information relating to a student's use and completion of the courses

1.2. Clause headings shall not affect the interpretation of this Data Sharing Agreement.

1.3. Capitalised terms used in but not otherwise defined in this Data Sharing Agreement shall have the meaning given to them in the Data Protection Legislation.

1.4. A reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time and shall include all subordinate legislation made from time to time under that statute or statutory provision.

1.5. Any words following the terms **including**, **include**, **in particular** or **for example** or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.

1.6. A reference to writing or written includes e-mail.

2. COMMENCEMENT AND DURATION

2.1. This Data Sharing Agreement shall take effect from the Effective Date and shall continue until its termination in accordance with clause 8.

3. COMPLIANCE WITH DATA PROTECTION LEGISLATION

3.1. The parties agree to comply with the Data Protection Legislation during the term of this Data Sharing Agreement. This clause is in addition to, and does not replace, a party's obligations under the Data Protection Legislation.

4. DATA SHARING

4.1. The parties acknowledge that for the purposes of the Data Protection Legislation, they are each independent Controllers for the Agreed Purpose. Where Up Learn is deemed to be the Customer's Processor, the terms of clause 6 shall apply

4.2. Each party shall:

4.2.1. ensure that it has a legal basis and all necessary consents and notices in place to enable the lawful transfer of the Shared Personal Data to the Permitted Recipients;

4.2.2. give full information to any Data Subject whose Personal Data may be processed under this Data Sharing Agreement of the nature of such processing, including that their Shared Personal Data may be retained by and transferred to one or more of the Permitted Recipients;

4.2.3. process the Shared Personal Data only for the Agreed Purposes;

4.2.4. not disclose or allow access to the Shared Personal Data to anyone other than the Permitted Recipients;

4.2.5. ensure that they have in place appropriate technical and organisational security measures to protect against unauthorised or unlawful Processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful Processing or accidental loss, destruction or damage and the nature of the data to be protected; and

4.2.6. ensure that all Permitted Recipients are obliged to keep the Personal Data confidential.

5. MUTUAL ASSISTANCE

5.1. Each party shall assist the other in complying with all applicable requirements of the Data Protection legislation. In particular, each party shall:

5.1.1. assist the other to respond to any request by a Data Subject to exercise their rights under the Data Protection Legislation, including promptly notifying the other if it receives any request by a Data Subject which may reasonably affect the other;

5.1.2. notify the other without undue delay of any Personal Data Breach;

5.1.3. upon the termination or expiry of this Data Sharing Agreement and at any time at the written direction of the other, delete or return the Shared Personal Data and any copies thereof to the other, unless required by the Data Protection Legislation or any regulatory requirement to continue to retain or store the Shared Personal Data; and

5.1.4. maintain complete and accurate records and information to demonstrate compliance with this Data Sharing Agreement.

5.2. Neither party shall retain, or Process Shared Personal Data for longer than is necessary to carry out the Agreed Purposes.

5.3. It is the responsibility of each party to ensure that it and its staff members are appropriately trained to handle and process the Shared Personal Data in accordance with the Data Protection Legislation.

6. PROCESSOR TERMS

6.1. In circumstances when Up Learn is processing Shared Personal Data on behalf of the Customer, this clause 6 shall apply.

6.2. Up Learn shall, in relation to any Shared Personal Data Processed by it on behalf of the Customer in connection with this Data Sharing Agreement:

6.2.1. Process that Shared Personal Data only on the written instructions of the Customer, as set out in Schedule 1, paragraph 3, or as otherwise agreed in writing, unless required otherwise by applicable law. If Up Learn is so required it will promptly inform the Customer before Processing the Shared Personal Data, unless prohibited from doing so by law;

6.2.2. notify the Customer immediately if it considers that any of the Customer's instructions infringe the Data Protection Legislation;

6.2.3. keep the Shared Personal Data confidential;

6.2.4. assist the Customer in responding to any request from a Data Subject to exercise their rights under Data Protection Legislation (as well as any relevant enquiry or complaint from such individuals in connection with their Shared Personal Data) and to ensure compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, privacy impact assessments and consultations with Supervisory Authorities or regulators;

6.2.5. notify the Customer without undue delay on becoming aware of a Personal Data Breach or communication which relates to the Customer's compliance with the Data Protection Legislation;

6.2.6. at the written request of the Customer, delete or return Shared Personal Data and any copies thereof to the Customer on termination of this Data Sharing Agreement

unless required by the Data Protection Legislation to store the Shared Personal Data; and

6.2.7. maintain complete and accurate records and information to demonstrate compliance with this clause and allow for audits by the Customer or the Customer's designated auditor.

6.3. Up Learn shall ensure that it has in place appropriate technical or organisational measures, to protect against unauthorised or unlawful processing of Shared Personal Data and against accidental loss or destruction of, or damage to, Shared Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures. Such measures may include, where appropriate:

6.3.1. pseudonymising and encrypting Shared Personal Data;

6.3.2. ensuring confidentiality, integrity, availability and resilience of its systems and services;

6.3.3. ensuring that availability of and access to Shared Personal Data can be restored in a timely manner after an incident; and

6.3.4. regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it.

6.4. In the event the Customer agrees, in writing, to the appointment of a sub-processor, Up Learn agrees to enter into a written agreement, which incorporates terms which are substantially similar to those set out in this clause 6, with the sub-processor. Up Learn shall remain fully liable for all acts or omissions of any sub-processor appointed by it.

6.5. Schedule 1, paragraph 3 sets out the scope, nature and purpose of the Processing by Up Learn of the Shared Personal Data, the duration of the Processing and the types of Personal Data and categories of Data Subject.

7. CROSS-BORDER TRANSFERS OF PERSONAL DATA

7.1. If an adequate protection measure for the international transfer of Personal Data is required under Data Protection Legislation (and has not otherwise been arranged by the parties) the Data Transfer Provisions shall be incorporated into this Agreement in the Schedules as if they had been set out in full.

7.2. The parties shall ensure that whenever Personal Data is transferred outside the European Economic Area and the United Kingdom, they:

7.2.1. are Processing Personal Data in a territory which is subject to a current finding by the UK's Information Commissioner's Office or European Commission (as applicable) under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals;

7.2.2. participate in a valid cross-border transfer mechanism under the Data Protection Legislation, so that the parties can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the GDPR; or

7.2.3. otherwise ensure that the transfer complies with the Data Protection Legislation.

8. TERMINATION

8.1. Each party reserves the right to terminate this Data Sharing Agreement with immediate effect if the other Party does not Process the Personal Data in accordance with this Data Sharing Agreement or breaches any other provision of this Data Sharing Agreement.

8.2. The parties shall review the effectiveness of this Data Sharing Agreement every 12 months from the Effective Date and, depending on the outcome of the review, shall make any necessary amendments to the Data Sharing Agreement.

9. GENERAL TERMS

9.1. **Assignment.** This Data Sharing Agreement is personal to the parties and neither party shall assign, transfer, mortgage, charge, subcontract, declare a trust of or deal in any other manner with any of its rights and obligations under this Data Sharing Agreement without the prior written consent of the other parties (which is not to be unreasonably withheld or delayed).

9.2. **Entire Agreement.** This Data Sharing Agreement and the documents referred to in it constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.

9.3. **Counterparts.** This Data Sharing Agreement may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement.

9.4. **Variation.** Except as expressly provided in this Data Sharing Agreement, no variation of this Data Sharing Agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

9.5. **Severance.** If any provision or part-provision of this Data Sharing Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this clause shall not affect the validity and enforceability of the rest of this Data Sharing Agreement.

9.6. **Third-party rights.** Except as expressly provided elsewhere in this Data Sharing Agreement, a person who is not a party to this Data Sharing Agreement shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Data Sharing Agreement. This does not affect any right or remedy of a third party which exists, or is available, apart from that Act.

9.7. **Governing law and Jurisdiction.** Except as set out in the Schedules, this Data Sharing Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of England and Wales. Each party irrevocably agrees that the courts of England shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Data Sharing Agreement or its subject matter or formation (including non-contractual disputes or claims).

SCHEDULE 1

EU SCCs

1 INCORPORATION OF THE EU SCCS

1.1.1 To the extent clause 6.1 applies and the transfer is made pursuant to the GDPR, this Schedule 1 and the following terms shall apply: Module 1 of the EU SCCs and no other optional clauses unless explicitly specified, are incorporated into this Schedule 1 as if they had been set out in full in the case where the exporter is a Controller, the importer is also a Controller and the transfer requires such additional protection.

2 CLARIFICATIONS TO THE EU SCCS

2.1.1 For the purposes of clause 8.2 of the EU SCCs and to enable Data Subjects to effectively exercise their rights, the parties have agreed that the exporter shall inform Data Subjects of the information required.

2.1.2 For the purposes of clause 8.3 of the EU SCCs the parties hereby agree that the exporter shall be primarily responsible for ensuring that Personal Data is accurate and, where necessary, kept up to date. The exporter shall take every reasonable step to ensure that Personal Data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

3 PROCESSING PARTICULARS FOR THE EU SCCS

The Parties

3.1 **Exporter (Controller):** Up Learn

3.2 **Importer (Controller):** the Customer

Description Of Data Processing

3.3 **Categories of data subjects:** Students, Parents

3.4 **Categories of personal data transferred:** the Shared Personal Data

3.5 **Sensitive data transferred:** Not applicable.

3.6 **Frequency of the transfer:** Continuous

3.7 **Nature and purpose of the processing:** for the Agreed Purpose

3.8 **Duration of the processing:** For the duration of the Agreement.

3.9 **Competent Supervisory Authority:** The Irish Data Protection Commissioner

3.10 **Technical and Organisational Measures:** [as per the Up Learn Information Security Policy] OR [As set out in Schedule 3]

SCHEDULE 2

UK ADDENDUM

1. Parties

As set out in Schedule 1.

2. Selected SCCs, Modules and Clauses

Module 1 of the EU SCCs and no other optional clauses unless explicitly specified, and as amended by the clarifications in Schedule 1, paragraph 2, but subject to any further amendments detailed in this Schedule 2.

3. Appendix Information

The processing details required by the UK Addendum are as set out in Schedule 1, paragraph 3.

4. Termination of the UK Addendum

In the event the template UK Addendum issued by the Information Commissioner's Office and laid before Parliament in accordance with s119A of the DPA 2018 on 2 February 2022, as it is revised under Section 18 is amended, either party may terminate this Schedule 2 on written notice to the other in accordance with Table 4 and paragraph 19 of the UK Addendum and replace it with a mutually acceptable alternative.

UP LEARN

SCHEDULE 3

Technical and Organisational Measures

1 Physical Access Controls

1.1 Measures that each party takes to restrict inappropriate access to personal data, and transfer of media and equipment on which personal data is stored, include:

- limit access to facilities where information systems that process personal data are located to identified authorised individuals;
- maintain emergency and contingency plans for the facilities in which its information systems that process personal data are located;
- personnel and subcontractors must obtain authorisation prior to storing personal data on portable devices, remotely accessing personal data, or processing personal data outside Supplier's facilities. This includes removing media (e.g., USB sticks and CD ROMs) and documents containing personal data from Supplier's facilities;
- maintain records of the incoming and outgoing media containing personal data, including the kind of media, the authorised sender/recipients, date and time, the number of media and the types of personal data they contain;
- use industry standard processes to delete personal data when it is no longer needed;
- restrict access to personal data in media leaving Supplier's facilities (e.g., through encryption);
- classify personal data to help identify it and to allow for access to it to be appropriately restricted (e.g., through encryption); and
- maintain an inventory of all media on which personal data is stored. Access to the inventories of such media is restricted to Supplier's personnel and subcontractors authorised in writing to have such access.

(a) Physical access controls:

- The party uses a central datacenter access request process with authorised approvers; and
- Users must use two-factor authentication (biometrics and access card) to gain entry to sensitive areas.

2 Technical access controls

2.1 Measures each party takes to restrict access to its data-processing systems include:

- use industry standard practices to identify and authenticate users who attempt to access information systems;
- maintain and updates a record of personnel and subcontractors authorised to access Supplier's systems that contain personal data;
- use industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage;
- store passwords in a way that makes them unintelligible while they are in force;
- identify those personnel and subcontractors who may grant, alter or cancel authorised access to personal data and resources;

- ensure that de-activated or expired identifiers are not granted to other individuals;
- ensure that where more than one individual has access to systems containing personal data, the individuals have separate identifiers/log-ins;
- Maintain industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed;
- de-activate authentication credentials that have not been used for six months;
- require that user sessions with access to personal data are automatically closed in case of non-activity during a predetermined period of time of no more than ten minutes;
- instruct users to log-off when leaving Supplier-controlled premises or when computers are otherwise left unattended;
- limit repeated attempts to gain access to the information system using an invalid password;
- Where authentication mechanisms are based on passwords, each party requires that the passwords are renewed regularly; and
- Where authentication mechanisms are based on passwords, each party requires the password to be at least eight characters long.

2.2 Technical access controls:

- Authentication mechanisms
  a) Connections to servers require dedicated credentials and the connection must originate from the Supplier's controlled premises which has both physical and logical access controls; and
  b) Protected network gear and other infrastructure devices requires access using a two-factor security token and password
- Password protections
  a) All passwords are converted to an obfuscated form using a one-way hash to prevent those with access to the authentication systems from deriving the actual passwords of other users; and
  b) Passwords must be changed according to a strict technical policy, or they will expire and become unusable.

3 Use controls

3.1 Measures each party uses to restrict individuals from accessing personal data to which they do not have access privileges include:

- maintain a record of security privileges of individuals having access to personal data;
- restrict access to personal data to only those individuals who require such access to perform their job function;
- log access and use of information systems containing personal data, registering the access ID, time, authorisation granted or denied, and relevant activity;
- security personnel verify the logs every month to propose remediation efforts to identify any irregularities in access or use and propose remediation efforts for such irregularities, if any; and
- personnel and subcontractors with access to personal data are subject to confidentiality

obligations.

3.2 Measures each party uses to keep unauthorised individuals from reading, copying, changing or removing personal data during processing and use or after storage include:

- controls to avoid individuals assuming access rights they have not been assigned to gain access to personal data they are not authorised to access; and
- anti-malware controls to help avoid malicious software gaining unauthorised access to personal data, in particular malicious software originating from public networks.

3.3 Use controls:

- The party uses role-based security to establish permissions and access to each set of assets;
- Access must be approved and granted by the designated asset owners;
- When an employee ceases to be employed by the party, access is removed on a timely basis

3.4 System Maintenance

- the use of antivirus software which is centrally managed and controlled including the deployment of regular virus definition updates; and
- security patches to be deployed within 30 days for high priority security patches, or immediately in the case of critical or emergent issues;
- Servers are scanned continuously for patch and antivirus compliance

4 Distribution controls

4.1 Measures each party uses that are designed to prevent unauthorised reading, copying, changing or removing of personal data during transmission or storage on media include:

- encrypt personal data that is transmitted over public networks;
- track disclosures of personal data, including what data has been disclosed, to whom, and at what time; and
- impose restrictions on printing personal data and has procedures for disposing of printed materials that contain personal data.

4.2 Asset classification and handling

- Print services do not run within the production environment – personal data to be printed must go through centralised security measures including physical access to printers and output material; and
- Employees with access to personal data are required to take training on the proper handling of personal data.

5 Input controls

5.1 Monitoring and logging measures each party uses to audit inputs, changes, and deletions from its data-processing systems include:

- logs the use of its data-processing systems containing personal data;
- Logs include ID, time, authorisation granted or denied, and relevant activity; and
- security personnel verify logs every six months to propose remediation efforts to identify any irregularities in access or use and propose remediation efforts for such irregularities.

5.2 Input controls:

Logical access controls

- Access to all personal data assets is granted through role-based security measures; and
- Event logging provides an audit trail regarding access attempts (both successful and failed).

6 Purpose controls

6.1 Measures each party uses to limit processing it performs as a data processor to only processing in accordance with the instructions of the data controller include:

- restrict internal testing efforts with actual personal data;
- When the party does use actual personal data for testing, it provides, and documents, the relevant level of security for the processing;
- back up any actual personal data prior to using it for testing;
- use security logs only for their intended security purpose;
- When the party is engaged to process special categories of data, the party maintains logical separation between this data and other data; and
- Technical support personnel and subcontractors only have access to personal data when needed.

6.2 Purpose controls: Separation of environments

- The party policy requires that test and production environments be physically and logically separated; and
- Network access control lists (ACLs) and firewall rules are in place to prevent cross-communication of environments.

7 Availability controls

7.1 Measures each party uses to protect against accidental destruction or loss of personal data include:

- do not initiate any data recovery procedures without the written authorisation of the Microsoft.
- redundant storage and its procedures for recovering personal data are designed to attempt to reconstruct personal data in its original state from before the time it was lost or destroyed.
- Use a variety of industry standard systems to protect against loss of personal data due to power supply failure or line interference.
- back up copies of personal data at least once a week, unless no personal data has been updated during that period.
- stores backup copies of personal data and recovery procedures in a different place from where the primary computer equipment processing the personal data is located.
- has specific procedures in place governing access to backup copies.
- log personal data restoration efforts, including the person responsible, the description of the restored personal data and which data (if any) had to be input manually in the recovery process.

- review recovery and backup procedures at least every six months.
- maintain procedures designed to allow for recovery of personal data within seven days.

7.2 Backup security controls

- Backups are encrypted to prevent unauthorised disclosure.
- Secure transport to the off-site storage facility is performed by a vetted and authorised security service supplier.

8 Administrative controls

8.1 Measures each party uses to document and track administrative oversight include:

- maintain security documents describing its security measures and setting out the relevant procedures and responsibilities of Supplier's personnel and subcontractors who have access to personal data.
- maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering personal data.
- appoint one or more security officers responsible for coordinating and monitoring the security rules and procedures.
- perform a risk assessment before processing the personal data or launching the Services.
- retain its security documents for at least five years after they are no longer in effect.

8.2 Security policies and standards

- Security policies and standards are approved and reviewed annually by executive management.
- The party has a team designated to engage on all security incidents to provide triage, remediation, and notification services.

9 Training

9.1 Each party informs its personnel and subcontractors about relevant security procedures and their respective roles. Each party also informs its personnel and subcontractors of possible consequences of breaching the security rules and procedures. Additionally:

- Each party only uses anonymous personal data in training.

9.2 Training requirements

- Staff must complete the yearly security training program.
- Security policies and standards are available to all party's personnel and subcontractors.
- Privacy training is made available to engineering, support and operations personnel and subcontractors responsible for privacy compliance.