Schedule B – Details required under Annexes and Table 1 to the SCCs

Set of SCCs no. 1: RM Ed as data exporter and RMESI as data importer;

The Standard Contractual Clauses Prescribed Provisions set out in Schedule A are hereby incorporated in these SCCs.

Annex I to the EU SCCs

A. LIST OF PARTIES

Data exporter(s):

1. Name: RM Education Limited (company number 1148594)

   Address: 142b Park Drive, Milton Park, Abingdon, Oxfordshire OX14 4SE

   Contact person's name, position and contact details: Data Protection Officer, dataprotection@rm.com and Willans Data Protection Services (RM's representative in the EU) of 2 Pembroke House, 28-32 Upper Pembroke Street, Dublin, Ireland D02 EK84. Email: https://www.willansdataprotectionservices.com/make-a-data-request/ Telephone: 00 353 1 447 0402.

   Activities relevant to the data transferred under these Clauses: The provision of products and services to its Customers

   By signing the below, the data exporter agrees to enter into the SCCs as stated in this document and in Schedule A.

Signature	
Name	Mark Cook
Title	Director
Date	31/07/2023

   Role (controller/processor): Processor

Data importer(s):

1. Name: RM Education Solutions India Pvt Ltd (company number 015931)

   Address: Unit No.8A, Carnival Techno Park, Kariyavattom PO, Trivandrum -695581, Kerala, India

   Contact person's name, position and contact details: Data Protection Officer, dataprotection@rm.com

   Activities relevant to the data transferred under these Clauses: Provision of support and data processing services to RM Education Ltd

   By signing the below, the data importer agrees to enter into the SCCs as stated in this document and in Schedule A.

Schedule B – Details required under Annexes and Table 1 to the SCCs

Signature	
Name	31/07/2023
Title	John Baskerville
Date	31/07/2023

Role (controller/processor): Processor (sub-processor)

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Students;

Users including:

- employees and staff of educational establishments, professional organisations, government agencies or other customers, and
- examiners, assessors and supervisors of examinations,

Customers, e.g. individuals who purchase goods and services, either for themselves or for the organisation they work for.

Nature of the processing

The nature of processing will include (but will not be limited to) accessing, collecting, structuring, storing, altering, retrieving, using, amending, reporting and erasing the data for specific purposes.

Purpose(s) of the data transfer and further processing

The purposes of the processing will include the provision of products and services to Customers.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As set out in the relevant Customer contract.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Not applicable

Categories of personal data transferred

The list below includes all products and services provided by RM Ed. For categories of personal data transferred relating to a particular product and/or service, please refer to the relevant contract or terms and conditions for such product.

- Name

Schedule B – Details required under Annexes and Table 1 to the SCCs

- Username
- Gender
- Contact information
- Job role
- Organisation
- Financial information, e.g. order data
- Educational and assessment data (including, but not limited to, student responses, marks, examiner/teacher comments, student number, pupil data)
- Family data
- Numerical identifiers including NI number, NASS (National Asylum Support Service) number
- Date of birth and age
- Location data such as IP address
- Video footage
- Screenshots of PC or other device
- Country of birth / nationality data
- Language
- Free school meals (FSM) and Pupil Premium data
- Identification information such as a student card, passport or other ID
- Disclosure and Barring Service (DBS) Status (formerly CRB check), Children's Barred List check (formerly list 99)
- Employment data including salary details
- Qualifications data
- Any other personal data entered in the relevant software by the Customer and/or its users or collected by the data exporter during the Term of this Agreement.

Note that the list above is not exhaustive and may change from time to time as products and services evolve. Please email dataprotection@rm.com for an up-to-date list.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- Health information including, but not limited to, details of medical conditions, disability, Special Education Needs (SEN) status
- Ethnicity and related information
- Religion
- Biometric data
- Child protection information including care order details
- Education supervision order
- Behaviour incidents data
- Any other sensitive personal data entered in the relevant software by the Customer and/or its users or collected by the data exporter during the Term of this Agreement.

Note that the list above is not exhaustive and may change from time to time as products and services evolve. Please email dataprotection@rm.com for an up-to-date list.

Schedule B – Details required under Annexes and Table 1 to the SCCs

Restrictions and safeguards include the following:

- strict purpose limitation
- access restrictions (including access only for staff having followed training)
- keeping a record of access to the data
- restrictions for onward transfers
- additional security measures.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous

C. COMPETENT SUPERVISORY AUTHORITY

The Data Protection Commission.

Schedule B – Details required under Annexes and Table 1 to the SCCs

ANNEX II to the EU SCCs

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

This document is a high-level overview of RMESI's technical and organizational security measures. More details on the measures we implement are available upon request. RMESI reserves the right to revise these technical and organizational measures at any time, without notice, so long as any such revisions will not materially reduce or weaken the protection provided for personal data that RMESI processes in providing its various services. In the unlikely event that RMESI does materially reduce its security, RMESI shall notify its UK Stakeholders and Parent company RM Plc.

RMESI shall take the following technical and organizational security measures to protect personal data:

a) Organizational management and dedicated team responsible for the implementation, and maintenance of RMESI's ISO 27001 information security program.
b) Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to the RMESI organization, monitoring and maintaining compliance with RMESI defined policies and procedures, and reporting the condition of its information security and compliance to RMESI Management.
c) Maintain Information security policies and make sure that policies and measures are regularly reviewed and where necessary, improve them.
d) Communication with RMESI applications utilizes cryptographic protocols such as TLS to protect information in transit over public networks. At the network edge, stateful firewalls, web application firewalls, and DDoS protection are used to filter attacks. Within the internal network, applications follow a multi-tiered model which provides the ability to apply security controls between each layer.
e) Data security controls which include logical segregation of data, restricted (e.g. role-based) access and monitoring, and where applicable, utilization of commercially available and industry-standard encryption technologies.
f) Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).
g) Password controls designed to manage and control password strength, and usage including prohibiting users from sharing passwords.
h) System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review.
i) Physical and environmental security of server room facilities and other areas containing confidential information designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of RMESI facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.
j) Operational procedures and controls to provide for configuration, monitoring, and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from RMESI possession.
k) Change management procedures and tracking mechanisms to designed to test, approve and monitor all changes to RMESI technology and information assets.
l) Incident / problem management procedures designed by RM Corporate IS and allow RMESI investigate, respond to, mitigate and notify of events related to RMESI technology and information assets.
m) Network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

n) Vulnerability assessment, patch management, and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.
o) Business resiliency/continuity and disaster recovery procedures, as appropriate, designed to maintain service and/or recovery from foreseeable emergency situations or disasters.
p) Formal Vendor Management program, including vendor security reviews for critical vendors to ensure compliance with RMESI Information Security Policies.
q) A Group Head of Security who is independent, regularly reviews Information Security risks and controls in place and report to RMESI Management at planned intervals. For breach notification, the Group Head of Security will coordinate with RMESI Management and liaise with Data Protection Officer (DPO) of RM for necessary actions to be taken.

Initial Release: September 9th, 2021

ANNEX III to the EU SCCs

LIST OF SUB-PROCESSORS

The data importer does not use any sub-processors.

ANNEX IV to the EU SCCs

DATA TRANSMISSIONS SUBJECT TO THE SWISS FADP

Supervisory Authority

The competent supervisory authority in Annex I.C according to Clause 13 for a data transfer that is exclusively subject to the Swiss Federal Act on Data Protection (**FADP**) is the Federal Data Protection and Information Commissioner.

Place of Jurisdiction for Actions Brought by Data Subjects

The term "Member State" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of claiming their rights in their place of habitual residence (Switzerland) in accordance with clause 18c.

Supplement Until the Entry into Force of the revFADP

The SCC also protects the data of legal entities until the revised FADP comes into force.

Schedule B – Details required under Annexes and Table 1 to the SCCs

Information Commissioner's Office

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

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

Part 1: Tables

(A) Table 1: Parties

Start date	Date of signature of this Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	See Annex IA. of the EU SCCs.	See Annex IA. of the EU SCCs.
Key Contact	See Annex IA. of the EU SCCs.	See Annex IA. of the EU SCCs.
Signature (if required for the purposes of Section 2)	Refer to the signature block of the EU SCCs.	Refer to the signature block of the EU SCCs.

(B) Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to including the Appendix Information.

(C) Table 3: Appendix Information

Schedule B – Details required under Annexes and Table 1 to the SCCs

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Annex IA. of the EU SCCs
Annex 1B: Description of Transfer: See Annex IB. of the EU SCCs
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II. of the EU SCCs
Annex III: List of Sub processors (Modules 2 and 3 only): See Annex III. of the EU SCCs

(D) Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19**Error! Reference source not found.**: ☒ Exporter