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

Set of SCCs no. 2: RM Ed as data exporter and SoNET 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

   Signature and date:

   Mark Lagler, Director

   13 December 2022

   Role (controller/processor): Processor

Data importer(s):

1.Name: SoNET Systems Pty Ltd (hereinafter "SoNET")

Address: Suite 2.02, 179 Queen Street, Melbourne, Vic 3000, Australia

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

Signature and date: John Baskerville, Director

14/12/2022

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

Name of sub-processor	**Subject matter**	**Nature of the processing**	**Duration of the processing**	**Location of the processing**
Atlassian (Jira)	Provision of issue tracking software (internal to the Provider)	Providing services to the data importer. The data importer may store personal data relating to tickets raised using the software.	Duration of the agreement between Atlassian and the data importer.	US, EU and Australia
Security Shift	Provision of implementation and support services relating to hosting infrastructure.	The data importer may be able to, and occasionally may need to, access personal data in order to provide the services.	Duration of the agreement between Security Shift and the data importer.	Australia

Categories of personal data transferred

The list below only relates to assessment services provided by SoNET.

- Name
- Username
- Gender
- Contact information
- Job role
- Organisation
- Educational and assessment data (including, but not limited to, student responses, marks, examiner/teacher comments, student number)
- Numerical identifiers
- Date of birth and age
- IP address

- Any other Data entered in the relevant software by the Customer and/or its users or collected by the Main Processor during the Term of this Agreement.

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
- Biometric data

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

General measures within SoNET

SoNET is both ISO/IEC 27001:2013 and ISO 9001:2015 certified. All relevant information assets are securely maintained in Amazon Web Services (AWS). All access to information assets is governed by SoNET's access control and acceptable use policies. SoNET employees are contractually bound to adhere to SoNET's policies.

Raising employee awareness

All SoNET employees are required to attend data security training in their first 3 weeks on the job, and subsequently receive periodic supplemental data security training. SoNET regularly sends all employees periodic data security awareness messages whose content changes based on current risks.

Security organization

SoNET has an information security group within the Information Technology area. The security group ("Information Assurance") monitors information assets for attacks and for various anomalies. The security group also conducts regular vulnerability assessments in addition to penetration tests. Employees outside the group are required to report security incidents to the Information Security Committee who governs all information security related matters. The reported incidents are handled in accordance with SoNET's incident management policy.

Technical and organizational measures within SoNET

The transferred data will be processed within the relevant AWS data center or other hosting environment (as may be the case), which is a professional-grade, locked and monitored facility with no physical access to the data. In order to ensure the confidentiality of the data, the following measures are implemented:

Entrance control

The access of unauthorized persons to AWS and to the data processing systems is denied through the following measures:

- Data centre physical access is only allowed for AWS approved employees. Refer section Physical Access under AWS Data Centre Controls (https://aws.amazon.com/compliance/data-center/controls/)

Access to systems

The unauthorized use of the data processing systems is prevented by the following measures:

- Specified user account for selected employees assigned
- Segmented secured access to the development environment with multi-step authentication
- Secured admin access with multi-factor authentication
- Dedicated environment for sensitive systems
- Access restrictions by user-groups, virtual devices and AWS security groups.

Access to data

Only authorized persons can process and use the data released to them, while unauthorized persons can neither read nor modify this data. For this purpose, the following measures are taken:

- Restrictive assignment of administrator rights
- Role Concept
- Encryption of data in transit

- Secure deletion of data
- Authorization rules
- Strict password policies
- Regular review of access rights
- Changes to data objects in the environment as well as through the application are logged
- Non-production data for software developers and testers.

Authorized persons

The access to the systems is regulated by different user levels with different rights adapted to them:

- **Administrators**: The Administrators group has access to all resources. The systems are administrated exclusively by the IT department and limited to trusted individuals.
- **Selected Senior Software Developers**: Selected Developers may be given temporary access to the resources needed to perform releases or diagnose faults.
- **Selected users**: The project staff entrusted with the further processing is provided with the necessary data to fulfil their work and to process the collected data.

Data separation

The separate processing of collected data for different purposes is ensured by:

- Separation of production and test system
- Logical data separation
- Differentiated authorizations for data management
- Differentiate administrative tasks in data management

Malware protection

Each client has Antivirus-Software installed. Automatic updates are enabled and managed by the IT department. Servers in AWS are

- all Linux based that have been hardened as per the Australian Signals Directorate recommendations for Linux and
- have real time analysis of logs and alerting provided through a SIEM to warn of unusual activity in the environment;
- Data imported into the system by end users is passed through and stored on S3 not the webservers. Uploaded files are not stored in any location that can be executed by the web servers.
- Protected by a WAF service
- Patched regularly

The security-relevant updates and patches published for all operating systems, all installed drivers and programs are regularly reviewed and installed (when applicable) on all IT servers.

Backup and restore

The data is backed up with AWS automated point-in time backups. This allows restoring the data to a specific time in the past. Data recovery has been tested. As an additional measure, data is synchronised with a secondary database. A disaster recovery/business continuity plan exists to recover from the AWS point-in-time backup or the secondary database should the data becomes inaccessible. The AWS Elastic Load Balancer is configured to automatically redirect end users to a healthy availability zone should an availability zone becomes unavailable.

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

Data Security Policy's "Computer System Security Requirements", reproduced below verbatim
SoNET maintains a computer security system that generally provides the following controls when technically feasible:

a) Secure user authentication protocols including:

- control of user IDs and other identifiers;
- a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as token devices;
- control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
- restricting access to active Users and active User accounts only; and
- blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.

b) Secure access control measures that:

- restrict access to records and files containing Strictly Confidential and Confidential information to those who need such information to perform their job duties; and
- assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.

c) Encryption of all transmitted records and files containing PI that will travel across public networks, and encryption of all data containing PI to be transmitted wirelessly.
d) Reasonable monitoring of systems, for unauthorized use of or access to PI.
e) No PI stored on laptops nor other portable devices.
f) For files containing PI on a system that is connected to the Internet, reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the PI.
g) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
h) Education and training of employees on the proper use of the computer security system and the importance of data security.

ANNEX III to the EU SCCs

LIST OF SUB-PROCESSORS

See the description of transfers to (sub-) processors in Annex IB above.

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 **Error! Reference source not found.**: ☒ Exporter