

Data processing addendum to the CASPA licence agreement

Between: _____ <organisation> of
_____ <address> (the "Data Controller")

and RSE Insight Limited, PO Box 162, Alresford, SO24 4BD (the "Data Processor")

Definitions

"GDPR" means EU General Data Protection Regulation 2016/679.

The terms, "data controller", "data processor", "data subject", "personal data", "sensitive personal data", "processing" and "personal data breach" shall have the same meaning as in the GDPR.

Subject matter and duration of the processing of Data Controller personal data

This addendum relates exclusively to the data recorded by the Data Controller within the CASPA product licensed from the Data Processor that is transferred to the Data Processor and applies only whilst a valid CASPA licence is held by the Data Controller.

The nature and purpose of the Processing of Data Controller Personal data

In normal use of CASPA, personal data and sensitive personal data recorded within the CASPA installation of the Data Controller is not shared with the Data Processor and the Data Processor cannot access the Data Controller's IT infrastructure on which CASPA is installed.

This addendum therefore relates exclusively to situations where, if a CASPA technical support issue cannot be resolved by guidance via email or telephone, files from or relating to the CASPA installation of the Data Controller may be required in order to allow the Data Processor to attempt to replicate an error, to amend data files that are corrupted or have been modified in error, or to otherwise assist in resolving the issue.

Such files may include database files from CASPA, files containing data the Data Controller is attempting to import into CASPA and files containing data exported from CASPA. In all cases, these files may contain personal data and sensitive personal data.

Refer to the CASPA website (<http://www.caspaonline.co.uk/key-features/gdpr/>) for more information about normal operation of CASPA and about managing CASPA support queries where data files may need to be transferred to the Data Processor and with respect to the GDPR.

The types of Data Controller personal data to be processed

Where CASPA database files are transferred to the Data Processor, the types of data may include, but are not limited to the following categories of Personal data:

- **Pupils:** First name, last name, UPN, date of birth, gender, admission number, categories of special education need, free school meals status, looked after status, pupil premium eligibility, first language, ethnicity, notes, results and targets, evidence
- **CASPA Users:** First name, last name, email address, telephone number

Where other files are transferred to the Data Processor, it is the responsibility of the Data Controller to ensure no other data types are supplied to the Data Processor. If sent, the Data Processor will be obliged to destroy the files and request the correct data.

The categories of data subject to whom the Data Controller personal data relates

- Pupils who are or have been recorded by the Data Controller within CASPA.
- Users of CASPA for whom CASPA user accounts have been created.

The Data Processor shall:

1. Process the Data Controller's data only on the written instructions of the Data Controller.
2. Take appropriate measures to ensure the security of processing and ensure that the people processing the data are subject to a duty of confidence. Storage and processing of the data shall only take place on the Data Processor's IT infrastructure which is accessible only by employees of the Data Processor and is secured against unauthorised access.
3. Only engage sub-processors with the prior consent of the Data Controller and under a written contract.
4. Promptly notify the Data Controller if it receives a request from a data subject and not respond to that request.
5. Provide reasonable assistance to the Data Controller to:
 - assist the Data Controller in providing subject access and allowing data subjects to exercise their rights under the GDPR.
 - assist the Data Controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments.
 - submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and 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.
6. Destroy personal data within two working days of resolution of the incident that caused the data to be transferred by the Data Controller to the Data Processor.

The Data Controller shall:

1. Warrant that explicit consent has been obtained from data subjects that their personal data and sensitive personal data recorded in CASPA could be transferred to the Data Processor.
2. Warrant that their processing and transfer of personal data will be carried out in accordance with the relevant provisions of the data protection law in force in the UK at the time of the transfer of data to the Data Processor.

Data Controller

Name:

Title:

Signature:

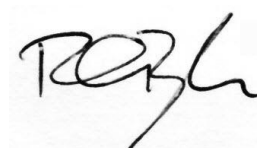
Date Signed:

Data Processor

Name: Roland Bugler

Title: Director

Signature:



Date Signed: 13th March 2018