

# CASPA and the General Data Protection Regulation (GDPR)

A joint statement by RSE Insight Ltd and SGA Systems Ltd

## Introduction

The General Data Protection Regulation comes into force on 25<sup>th</sup> May 2018 and replaces the Data Protection Act.

This document aims to provide the information that the DfE has suggested schools need from their IT suppliers in order to prepare for GDPR. It covers the normal operation of CASPA.

In rare situations, data from CASPA may be required to allow RSE Insight Ltd to resolve support issues raised by the User. For information on the terms under which RSE Insight Ltd would process such data, please refer to [‘Processing of personal data to provide technical support for CASPA under the GDPR’](#).

## What is CASPA and how is it used?

CASPA is a software system that allows educational establishments (the User) to record, analyse and benchmark attainment and progress. CASPA is installed by the User on the User’s IT infrastructure. All data recorded in CASPA or exported by CASPA is under the control of the [Data Controller](#) appointed by the User. Neither RSE Insight Ltd nor SGA Systems Ltd can access the User’s CASPA data and there is no processing of data under the terms of your CASPA licence by either RSE Insight Ltd or SGA Systems Ltd that would make either organisation a [Data Processor](#).

## SCOPE: what data can be recorded in CASPA and who decides what is recorded?

The data recorded in CASPA is entirely at the discretion of the Data Controller; CASPA has features to record both [Personal Data](#) and [Sensitive Personal Data](#)

## SHARING: what flows of data into and out of CASPA do I need to track?

CASPA has a number of features for the import and export of data, the use of which is at the discretion of the Data Controller; there are two distinct categories of data flow as noted below:

- **Export of anonymised data for analysis.** The data in this export is fully anonymised and is therefore not considered personal data under the terms of the GDPR.
- **All other imports and exports of data.** These data transfers may include both personal and sensitive personal data. All import or export of data requires initiation by a user of CASPA and exports will result in data being exported to a file on your infrastructure. Onward transmission or dissemination of that data is entirely at the discretion of the Data Controller.

## **RETENTION: how long is data retained for and who decides?**

CASPA is intended for the long-term tracking of pupil progress, including historic progress which may include the progress of pupils no longer on roll. CASPA does not enforce a data retention policy, and all decisions relating to the retention of data are at the discretion of the Data Controller

## **ACCESS: how would the data required for a data subject access request be prepared?**

We will provide details on request as to how the information in CASPA relating to an individual (data subject) can be extracted in order to respond to a data subject access request.

## **SECURITY: how does CASPA ensure the security of the personal data it holds?**

When considering the security of the data, there are a number of considerations; how is the data physically protected, who can access the application and what steps are in place to prevent unauthorised processing and, in the case of a breach of physical protection of the data, how are the data files themselves secured.

- **Physical security.** Security of the IT infrastructure and buildings where CASPA is installed and accessible from is under the control of the User and the Data Controller; neither RSE Insight Ltd nor SGA Systems Ltd can remotely access your CASPA installation
- **Control of the application.** Access to CASPA requires a user account and password; each user account is assigned a CASPA role that defines its privileges within CASPA; the most sensitive operations require re-validation of account credentials; the management of CASPA accounts and access arrangements is entirely under the control of the Data Controller.
- **Underlying data security.** All data files that form part of a CASPA installation are encrypted and users are not provided with the decryption key under any circumstances. Exports and reports generated by CASPA are in general not encrypted and, since they are all user-generated, are the Data Controller's responsibility to secure

## **OWN READINESS: will the supplier be GDPR compliant by May 2018?**

RSE Insight Ltd expects to be GDPR compliant where it acts as a Data Processor under contract to the school for specific actions relating to technical support, fault-finding, etc. for CASPA as described in the separate document ('Processing of personal data to provide technical support for CASPA under the GDPR'). As noted earlier, neither SGA Systems Ltd nor RSE Insight Ltd act as Data Processors in respect of personal data recorded in CASPA in any other circumstances.

Both SGA Systems Ltd and RSE Insight Ltd expect to be GDPR compliant as Data Controllers for the use of Personal Data in their respective normal business activities, including names and contact details provided that relate to the purchase and support of CASPA. For further information, please refer to RSE Insight Ltd's Privacy Notice and SGA Systems Ltd's Privacy Notice which will be made available in due course.