

GDPR Questions Answered from the DfE of MIS Suppliers



|  |  |  |  |
| --- | --- | --- | --- |
| **Document Ref:** | *GDPRDFE* | **Version:** | *1.0* |
| **Document Author:** | *Elaine Smith* | **Valid from:** | *6.2.2018* |

|  |  |  |
| --- | --- | --- |
| **Contact:** | *Pennine Education Ltd* | e-Mail:esmith@pennineeducation.co.uk |

The DfE have suggested six questions schools should ask of their MIS Suppliers, this is Capita SIMS responce

06/02/2018

**What are the areas the DfE are asking schools to challenge their MIS suppliers?**

The DfE are starting to address school’s concerns over the forthcoming GDPR regulations that come into effect this May. They have started with a [GDPR Blog](https://teaching.blog.gov.uk/2017/10/24/general-data-protection-regulation-evolution-or-revolution-for-schools) and [Video on YouTube](https://youtu.be/y09IHXv6u6M), but have also suggested schools review the following areas and challenge their MIS suppliers as needed:

SCOPE | SHARING | RETENTION | ACCESS | SECRUITY | OWN READINESS

**SCOPE: Which data items classed as sensitive or highly sensitive under GDPR are contained within that system?**

Firstly let’s distinguish between personal (sensitive) and highly sensitive (special category) data. The [ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/) defines these as:

[Personal Data](https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/) means data which relate to a living individual who can be identified

* from those data, or
* from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be “personal data”.

[Sensitive personal data](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/) updated for GDPR means personal data consisting of information as to

* race
* ethnic origin
* politics
* religion
* trade union membership
* genetics
* biometrics (where used for ID purposes)
* health
* sex life
* sexual orientation

SIMS allows users to add in all this information if they wish either in the fields provided or as customisable user defined fields **with the exception of biometric data**, i.e. finger print or iris recognition.

**SHARING: Does any sensitive personal data flow from that system onto anywhere else that I need to track to fully understand my personal data ecosystem?**

In the first of a series of videos from the DfE (2), Iain Bradley discusses understanding your data ecosystem and mapping where you store, control and process data. SIMS allows partner products to interact with our database, a school will have a contract with those partner products and as such should challenge them as to the data they extract and process. The school is the data controller in this case and the partner will be the processor.

We advise schools to review the system manager access permissions granted to the various partner SIMS user ID’s to ensure they only have access to the data you expect.

**RETENTION: What is the data retention policy of this system? Does it align to the data retention policies I need to fulfil my duties as a school, and is this clear within my contractual relationship with the supplier?**

Many of our customers will be using additional products from Capita such as the Teacher, Parent and Student Apps. Each of these satellite products have their own Privacy Statements detailing this and much more about their use of the data. All of these can be found in our [GDPR Hot Topic.](https://myaccount.capita-cs.co.uk/hot-topics/sims-gdpr/)

When it comes to enforcing a data retention policy for the core SIMS application, schools will each individually have different advice and guidance so it’s impossible for us to allow a school’s data controller to manage their retention periods. At this time a user can delete data from student’s records on a row by row basis. This summer we are planning to introduce enhanced functionality where users can bulk delete parts of a selection of students record, e.g. for students who left in the academic year 2010/2011 or prior, delete all their conduct data, other data domains will be made available to a point where you will just be left with the basic pupil record. At this point, the school will then be able to bulk delete all those records in one go.

Once we have delivered this facility for students, we can review the same process for staff. It’s likely that the functionality for staff will be delivered in the Autumn 2018 release of SIMS.

**ACCESS: How would I go about getting the information relevant for a subject access request out of the system?**

In the [SIMS Autumn 2017 release](https://myaccount.capita-cs.co.uk/Notifications/GDPR-SAR-SIMS/) we introduced the Student Person Data Output (PDO) report. A [video demonstration](https://www.capita-sims.co.uk/resources/videos/how-sims-can-help-your-school-comply-gdpr) is available for viewing on the Capita SIMS website. This report is designed to output in one report nearly all of the student’s data in one go. Where there is a lot of individual pieces of data, such as sessional attendance data, we summarised this data by attendance mark type for each academic year. If the user wishes to have the individual sessional marks, we have existing registration certificates that can be generated to supplement the PDO report.

In the Spring 2018 release of SIMS we extend this functionality to cover Staff and Contacts.

**SECRUITY: How does the system ensure the security of the personal data held? What recognised standards are in place?**

The security of SIMS can be broken down into two themes. Firstly the data controller determines which users have access to SIMS and at what level. SIMS enables schools to use pre-defined permission groups, or if they wish, they can create their own custom permission groups. The data controller can at any point add or remove an individual’s membership to the permission groups to fit the role of that person and the data they should have access to. Secondly the data controller must ensure that the SIMS Database is being sufficiently secured within their school, e.g. does the network server where the SIMS database is being stored have up to date anti-virus and malware protection, is the server in a secure location to prevent theft? If SIMS is on premise, then this will be the responsibility of the data controller.

If a SIMS Support Unit, Private Company or Capita itself are hosting SIMS on behalf of the school, then there is a greater responsibility on the data processor to ensure data is secure. Capita Hosted SIMS customers can request assurances on this matter via the SIMS Service Desk.

**OWN READINESS: Is this system supplier confident that it will be GDPR compliant by May 2018? How will they demonstrate this to me?**

We are confident that SIMS will be in a strong position to help schools be GDPR compliant by May 2018. We have outlined in our [GDPR Hot Topic](https://myaccount.capita-cs.co.uk/hot-topics/sims-gdpr/) our plans to improve particular areas of our software and we recommend that customers keep a close eye on this Hot Topic for any future updates.