

SIMS Student Privacy Statement

We take care to protect the privacy of customers and users of Capita websites. Set out below is an explanation of how we process information about visitors to the site.

SIMS Student

SIMS Student is designed to give students access to key information about their school lives. Designed with input from schools, parents and students, SIMS Student is intuitive and informative, providing students with the information they need to ensure they are getting the most out of school life.

What Information is Transferred?

SIMS Student depends on data that is held within the SIMS system. For example, student data is displayed within SIMS Student to contextualise the applications' functionality (e.g. forename, surname, and student/parent relationships).

Selected information is transferred to SIMS Student periodically, via the SIMS Online Services Client over a secure channel. The SIMS Online Services Client (school-side) uses client credentials to uniquely identify the school and authorise at the server

The following data is required to allow the school to invite Students to use SIMS Student and to display relevant data to students. Configurable items will only be stored if they have been enabled by the school administrator:

Item	Data Fields	Configurable
Student Data	Forename, Surname, Date of Birth, School Photo	No
School Details	Address, Head Teacher, Email Address, Web Site, Phone Number, Academic Year	No
Homework	Title, Description, Subject, Created By, Start Date, Due Date, Handed In Date, Comments, Result, Status	Yes
Timetable	Subject, Room, Teacher, Start Time, End Time, Classes	No
School Diary	Description, Category, Start Time, End Time	No

Where is the Data Stored?

Data is stored within SIMS Student in various forms, all using Microsoft Azure data constructs. Information interchange between software services within the applications is protected by a dedicated Secure Token Server (STS), so that access to all data is validated against the access rights of the requesting user.

Data sits with the EEA and is subject to EU model clauses, specifically data for these services reside in the EU: Ireland and the Netherlands.

Security of the Data Stored

SIMS Student is a securely hosted web service, delivered via the web using standard HTTPS TCP/IP protocols. The SIMS Student application is hosted on a secure and highly scalable managed service, with the main system hosting provided by Microsoft Azure UK, which is reliable and resilient. Microsoft Windows Azure has G-Cloud Impact Level 2 (IL2) from the Cabinet Office for use across the UK Public Sector. All data is securely stored and processed within the EU and complies with UK data protection standards and requirements.

Technical hosting and management for SIMS Student is undertaken fully by Capita on behalf of the establishment, including the provision of all software, maintenance operations, upgrades and background supporting processes. Application security is 256bit Secure Socket Layer (SSL), point-to-point encryption.

Where the Data is Processed

The SIMS Student application is hosted on a secure and highly scalable managed service, with the main system hosting provided by Microsoft Azure UK, which is reliable and resilient. Microsoft Windows Azure has G-Cloud Impact Level 2 (IL2) from the Cabinet Office for use across the UK Public Sector. All data is securely stored and processed within the EU and complies with UK data protection standards and requirements.

Is There Any Third Party Processing of the Data?

SIMS Student sends reminder notifications using the Apple Push Notification service and the Google Cloud Messaging service. These notifications contain summary information about Student events.

What Information from Sign-In Providers does Capita Receive and Store?

When a student user logs into the service via SIMS ID using a third-party login, they are prompted with a consent screen where they consent for their e-mail address and name to be passed to SIMS ID.

The e-mail address and name are passed to SIMS ID, but no extended properties are received except a unique identifier. The third-party ID provider has no concept of the education establishments that the user is associated with, however, SIMS ID and Student App understand the site context.

In the SIMS ID database the e-mail address and a unique identifier are stored. The third-party provider detail may include the student's provided name. This is not stored – SIMS ID stores a name associated with the student from Student App (SIMS People Service).

Is the Information Received from Third Party Providers used Outside of the Sign-In Process?

The information is used to associate the third-party account with the SIMS ID identity that is used to authenticate the user to Student App. The name from Student App is displayed to assist in identifying correct sign-in by the end user.

We do not store the email address provided by the third-party login provider. We do, however, store the email address provided from Student App during the initial invite process for audit purposes.

What Information do Sign-In Providers Receive from Capita?

No information is passed from Capita to the sign-in provider. We do not send credential information to the third-party provider. The information those service providers have already is freely given and agreed to at the point the user creates an account with the third party and has accepted the provider's terms and conditions. The customer is required to examine what they have signed up to in order to determine this.

Cookies Policy

The SIMS Student web application does not use cookies.

SIMS Student uses a small number of cookies to provide the features in the web site and to help us improve its performance.

If you do not know what cookies are, or how to control or delete them, then we recommend you visit <http://www.aboutcookies.org> for detailed guidance.

The list below describe the cookies we use on this site and what we use them for:

Cookie Name	Purpose
ai_authUser	This helps us to proactively analyse the performance of the site and its infrastructure
ai_session	This helps us to proactively analyse the performance of the site and its infrastructure
ai_user	This helps us to proactively analyse the performance of the site and its infrastructure
angular-consent.global	Used to track if cookies have been accepted

Changes to this privacy notice

We keep our privacy notice under regular review. This privacy notice was last updated on 27/10/2017.