Privacy Policy

Privacy Policy Updated / Reviewed February 2024

SAM Learning respects the privacy of its users and is committed to protecting your personal data. This privacy policy explains how we do this, and how it applies to your use of SAM Learning's website and services. SAM Learning is fully compliant with the General Data Protection Regulation, also known as the GDPR, a European Union regulation and also with the UK's Data Protection Act 2018.

- SAM Learning Ltd is a registered company, No. 2826785, with registered address Webber House, 26-28 Market Street, Altrincham, Cheshire, WA14 2DT
- SAM Learning is registered with the ICO: Z7116737
- All data is held within the EU
- You retain full control over what data we can access
- All data is transmitted using SSL/TLS encryption
- Data at rest is encrypted with AES
- All data is processed for the purpose of running SAM Learning
- All personal data is anonymised or deleted (your choice) at the end of the school's subscription – if we receive no instructions, we anonymise all data within 90 days

Downloads

- SAM Learning – Data Sharing Agreement
- SAM Learning – Legal Compliance Documentation
- Data Transferred Outside of the United Kingdom
- Groupcall – GDPR Statement

SAM Learning Data & Privacy Policy

This privacy statement covers your use of the website and related services provided by SAM Learning Ltd ('SAM Learning'). Specifically, this policy sets out what data is collected, how that data is used, how it is kept secure and how long it is kept. It also outlines your rights to access your data and how to contact SAM Learning for more information.

What data does SAM Learning require schools to share?

We require all schools to share learner first and last name, admission number, gender, date of birth, registration group, school year, unique pupil number (UPN), school email address and classes. This data is needed in order to properly provision learner accounts as well as SAM Learning services.

In addition to the above data, a school may choose to share data on the following learner characteristics: ethnicity, free school meals status, FSM6 status, pupil premium status, special education needs status, looked after children status, and English as an additional language status. This data is needed to allow filtering and analysis based on these learner characteristics. Specifically, this includes advanced functionality as listed:

- School Intervention groups to be created, as requested by the school's senior leader
- Advanced learner data filters for progress-monitoring enabled
- Teacher/senior leader detailed customised reports enabled, including an intervention-focus report

Teachers and senior leaders who wish to use SAM Learning are required to share their first and last name, job title, school role, email address, educational/subject interests and exam boards used. They are also linked to their timetabled classes data. This data is needed in order to properly provision teacher/admin accounts as well as SAM Learning services.

We also store the address and contact details of the school.

How is this data gathered by SAM Learning?

Learner data is shared one of three ways over which the school has full control:

- A School Data Manager installing and authorising WONDE or Groupcall XoD that, once set up, automatically syncs nightly to our secure servers by SSL 3.3/TLS 1.2 encryption (see Groupcall – GDPR Statement - WONDE - School Data & Information Security Overview)
- A Senior Leader manually uploading a data file to our secure servers by SSL 3.3/TLS 1.2 encryption (see SAM Learning – Data Sharing Agreement)

Teacher and senior leader data is either collected via WONDE, Groupcall XoD or inputted manually by the user as part of their registration process.

What is the lawful basis for storing this data?

This data is required for learners, teachers and senior leaders to be able to use the SAM Learning platform for assessment, learning, intervention, support, revision, classroom use and homework, in accordance with the school's contractual agreement with SAM Learning.

Where and how is this data stored?

The data is stored on SAM Learning's servers in data centres in Ireland, provided by Amazon Web Services (AWS). AWS data centres are compliant with the international information security standard, ISO 27001.

For more information about AWS's ISO 27001 certification, please visit this webpage.

For more information about AWS security, please visit this webpage.

In choosing AWS to store data, SAM Learning is subject to its Shared Responsibility Model. The division of these responsibilities and how SAM Learning specifically meets those responsibilities as an AWS customer is outlined below:

	Responsibility of SAM Learning	Responsibility of Amazon Web Services
Preventing or detecting when an AWS account has been compromised: ● Multi-factor authorisation is enabled ● Access key IDs and secret access keys are used in managing authorised access to SAM Learning's AWS account ● Change-monitoring software is in place to detect unauthorised access	x	
Preventing or detecting a privileged or regular AWS user behaving in an insecure manner ● Individual identities used to enable monitoring of each user's behaviour by system administrators ● Internal ISMS (Information Security Management System) in place, controlling access and permissions for each user ● Onboarding and offboarding protocols in place, controlling set-up and removal of users ● Credentials deactivated the same day as a user leaves the company	x	
Configuring AWS services (except AWS Managed Services) in a secure manner: ● TLS (Transport Layer Security): the SAM Learning platform is accessible only over SSL 3.3/TLS 1.2 encrypted connections ● Only specific IPs configured/authorised can access AWS server ● File System Encryption: keys and passwords are kept in an unreadable, encrypted closed format ● Platform, Applications, Identity and Access Management: maintenance and	x	

protection of the platform running on the cloud, and all aspects that fall under that		
Restricting access to AWS services or custom applications to only those users who require it - Customer Data Protection: only authorised users can access the data using the SAM Learning platform and only within the authorised scope (e.g the school) - Network Traffic Protections: only authorised IPs can access the AWS server	x	
Updating Guest Operating Systems and applying security patches - Security patches and updates are monitored by system administrators and applied regularly	x	
Ensuring AWS and custom applications are being used in a manner compliant with internal and external policies - All processes carried out by SAM Learning using AWS have been audited for GDPR compliance - All processes carried out by SAM Learning using AWS are in accordance with the AWS terms of use	x	x
Ensuring network security (DoS, MITM, port scanning) - Protection against MITM is provided by SAM Learning's SSL connections - AWS internal machines are not exposed to port scanning - In a Denial of Service situation, the server would become temporarily inaccessible without data loss	x	x
Configuring AWS Managed Services in a secure manner		x
Providing physical access control to hardware/software		x
Providing environmental security assurance against things like mass power outages, earthquakes, floods, and other natural disasters		x

Database patching		x
Protecting against AWS zero day exploits and other vulnerabilities		x
Business continuity management (availability, incident response)		x

Related to disaster recovery, how is data backed up?

Data is backed up daily by AWS Ireland data centres. All backups are encrypted and are stored for 30-days.

Is SAM Learning registered as a data controller with the ICO?

SAM Learning Ltd is registered as a data controller with the ICO under registration Z7116737.

How is data encrypted between the clients and your AWS servers? Which version(s) of SSL/TLS and other encryption are supported?

Data is encrypted using SSL 3.3 / TLS 1.2 encryption between clients and our AWS servers.

Are SAM Learning personnel police or DBS checked?

All SAM Learning personnel are DBS checked upon employment commencement. Additionally, all SAM Learning personnel are DBS checked/verified as part of internal HR processes and SAM Learning GDPR audit processes.

Do you share our school data with any third-party organisations?

We share limited data with our customer support software, ZenDesk, including teacher and senior leaders' names, school names and email addresses. This allows us to help with any technical problems or support requests quickly and easily, via email, by telephone or by an online chat system.

We do not share learner data with ZenDesk unless a learner emails us directly, in which case we store their first and last name, school name and email address. ZenDesk is based in the USA and this data transfer is covered by the EU-US Privacy Shield.

For more information, please visit the following two pages:

https://www.zendesk.com/company/customers-partners/eu-data-protection/

https://www.zendesk.com/company/customers-partners/eu-data-protection/#privacy-shield

For information regarding ZenDesk's GDPR compliance, please visit this page.

For our digital marketing (email campaigns) system, we use SendGrid and Apollo.io. We share limited data with SendGrid, including teacher and senior leader first and last names and email addresses. This allows us to send communications regarding any platform downtime, scheduled maintenance, new features/functionality, platform enhancements, implementation strategies and support services available.

Emails contain tracking facilities within the actual email. Tracked activities include: the opening of emails; the clicking of links within the email content; times, dates and frequency of activity; how you access and view the emails (web browser version, OS version). You have the right to opt out of digital marketing (email campaigns) at any time: you can opt out using the 'Unsubscribe' link at the bottom of each email we send or you can email DPO@samlearning.com and request to be removed.

For information regarding SendGrid's GDPR compliance, please visit this page.

For information regarding Apollo.io's GDPR compliance, please visit this page.

For our customer relation management system, we use Solve360 and store a history of your school's contractual relationship with SAM Learning, including subscription history, product history, MIS upload history and a record of communications with SAM Learning.

For information regarding Solve360's GDPR compliance, please visit this page.

For our accountancy system, we use Xero. We store school addresses, the name and email of our contacts (e.g. finance office), invoices/transactions, payment terms and payment history.

For information regarding Xero's GDPR compliance, please visit this page.

Lastly, we do share anonymised learner data with third-party organisations, like Fischer Family Trust (FFT) for educational statistical analysis only.

How long will the data be kept?

During the subscription period, if a learner becomes a leaver, their account and all associated data is anonymised within 90 days.

All personal data is anonymised or deleted (your choice) within 90 days after the school subscription ends – if we receive no instructions, we anonymise all data within 90 days.

Upon request, we can destroy a school's data within 24 hours.

How will the data be anonymised?

Learner, teacher and admin (senior leader) data will be anonymised as follows:

Learner Accounts will be anonymised as follows:

Learner first names are replaced with 'Anonymous' and last names are replaced with 'Learner-' along with a random string of 6 numbers/letters. For example, Albert Einstein would become ‘Anonymous Learner-BFHPIL’. This is carried out so that we can continue to improve our understanding of program efficacy and impact evaluation, while ensuring anonymity. Below is a full listing of learner data fields and treatments applied:

Original Data	**Data Treatment**	**Original Data**	**Data Treatment**
First Name	‘Anonymous’	**User ID**	Regenerated using new random DoB and Anonymised name
Last Name	‘Learner-’ + 6-character randomised string of numbers and/or letters	**Password**	Regenerated
Admission number	*Retained*	**Memorable question**	Deleted
Gender	Randomised	**Memorable question answer**	Deleted
Date of birth	Randomised (with parameter that new learner age must be between 7 and 40)	**SAM Learning activity scores**	*Retained*
Registration group	‘Reg group-’ + 6-character randomised string of numbers and/or letters	**SAM Learning points earned**	*Retained*
Year group	*Retained*	**Gamification: avatar and clothes**	Reset to default
Unique pupil number (UPN)	*Retained*	**Gamification: World buddies**	Deleted
Classes	‘Class-’ + 6-character randomised string of numbers and/or letters	**School email address**	Deleted

Teacher Accounts will be anonymised as follows:

Teacher first names are replaced with ‘Anonymous’ and last names are replaced with ‘Teacher-’ along with a random string of 6 numbers/letters. For example, Johnny Appleseed would become ‘Anonymous Teacher-HLZWQY’. Below is a full listing of teacher data fields and treatments applied:

Original Data	**Data Treatment**
First Name	‘Anonymous’
Last Name	‘Teacher-’ + 6-character randomised string of numbers and/or letters
Job Title	Deleted
Job Role	Deleted
Email Address	Deleted
Subject(s)	Link between teacher and subjects deleted
Exam boards used	Deleted
Classes	‘Class-’ + 6-character randomised string of numbers and/or letters
Intervention Groups	‘Group-’ + 6-character randomised string of numbers and/or letters
Tasks	‘Task-’ + 6-character randomised string of numbers and/or letters
User ID	Regenerated using Anonymised name
Password	Regenerated

Senior Leader Admin Accounts will be anonymised as follows:

For the school’s main Admin account, the username ‘Admin’ is retained. Senior leader first names are replaced with ‘Anonymous’ and last names are replaced with ‘Admin-’ along with a random string of 6 numbers/letters. For example, Johnny Appleseed would become ‘Anonymous Admin-VBXMPZ’. Below is a full listing of main admin account data fields and the treatments applied. Any additional teachers who have an account with admin permissions are treated the same as a standard teacher account (above).

Original Data	Data Treatment
First Name	‘Anonymous’
Last Name	‘Admin-’ + 6-character randomised string of numbers and/or letters
Job Title	Deleted
Email Address	Deleted
User ID	Retained as ‘Admin’
Password	Regenerated

On request we can delete all data, removing it from our servers completely.

What other information do you store about users once they use SAM Learning?

We store information about their use of SAM Learning.

For learners, we store their total platform usage (hours:minutes), activity history, activity scores, SAM Learning gamification points earned, gamification trophies earned, gamification avatar clothes selected and gamification SAM World buddies selected.

For teachers and senior leaders we store the date they last logged in, total number of logins since the beginning of the academic year, total number of tasks set, classroom intervention groups created and activities they have created using our authoring tool Activity Builder.

What is your policy for serious incidents such as data breaches?

Should a school or subject (user) report a serious incident, such as a data breach, or should a serious incident be identified by SAM Learning, we will notify the impacted school’s senior leader and any affected subjects within 48 hours.

Following SAM Learning’s internal data breach protocol, we will work closely with all subjects impacted to minimise the incident and ensure it is fully resolved.

To report a concern or possible incident involving SAM Learning, submit a support ticket, email DPO@samlearning.com or call SAM Learning Customer Support on 0845 130 4160 Monday-Friday from 8:00am to 5:00pm. Should any issue not be resolved, they can be escalated to the Founder, David Jaffa, via djaffa@samlearning.com.

What are cookies and how do you use them?

Cookies are small text files that are set by a website or app operator so that your browser or device may be recognised. Cookies track, save and store information about your interactions with and usage of a website.

SAM Learning uses cookies to optimise your experience on our website and provide you with a more tailored, improved experience. SAM Learning uses Google Analytics software to monitor website behaviour to enhance our service offering. This software will save a cookie to your device in order to track and monitor your engagement and usage of the website, but will not store, save or collect any personal information. You can read Google's privacy policy here for further information.

If you don't want cookies to be stored on your device, you should make the necessary changes to your device, relevant browsers or apps.

How can access be revoked for members of staff who have left a school?

For schools registering their staff manually, senior leaders with an active SAM Learning admin account can make a member of staff inactive, which will prevent them from having access to SAM Learning.

1. Sign into the SAM Learning admin account
2. Click 'Profile'
3. Click 'Teacher Data'
4. Find the member of staff from the list
5. Change the corresponding drop down from 'Active' to 'Inactive'
6. Click Save

For schools using WONDE or Groupcall XoD to supply teacher data, a list of active teachers will be synced daily from the school's Management Information System, e.g. SIMS and any teachers no longer present will automatically have their SAM Learning accounts deactivated. They will receive an email notification of this.

On request we can delete a teacher or admin account, removing the teacher/senior leader and their data from our servers completely, within 24 hours.

How can learner data be removed when the learner leaves the school?

If your school elected to manually upload learner data: at any time senior leaders with an active SAM Learning admin account can delete learner accounts using the Learners page of SAM Learning. This prevents those learners from accessing SAM Learning and immediately deletes all of that learner's data from our servers completely.

1. Sign into the SAM Learning admin account
2. Click 'Learners'

3. Find the learner from the list
4. Tick the corresponding checkbox next to the learner’s last name
5. Click ‘Delete Learner’ found at the bottom of the page
6. Confirm your selection
7. Click Yes

If your school elected to provision learner data via SIMS-sync or Groupcall XoD integration: during the subscription period, if a learner becomes a leaver, their account and all associated data is automatically anonymised within 90 days.

On request we can delete the learner, removing the learner and their data from our servers completely, within 24 hours.

How can I access my data?

A Subject Access request can be made by submitting a support ticket or by emailing DPO@samlearning.com. Upon authenticating the subject’s identity, we will provide all data we hold on the subject (or organisation) in a spreadsheet, within 30 days.