Schools UK GDPR Information

Name of Supplier:	Schools UK
Service Provided to the School/s:	Staff Absence Insurance and Wellbeing Services

Description of the data that is accessed/processed?	Schools UK store and access data relating to the school as well as school members of staff. Data includes claims, medical documents where required, insurance premiums and school contact details
Where is the data stored/recorded?	Schools UK use AWS (Amazon Web Services). The AWS datafarm is in Dublin, Ireland.
If the data is stored in a cloud based facility, where are the servers located?	The AWS datafarm is in Dublin, Ireland.
How long is the data retained for?	Data for schools is retained indefinitely unless deletion is requested. Data for individual members of staff and their claim information, medical reports etc are deleted 6 years after the claim has ended. Subject to underwriters
How and where is the data backed up?	Currently all the data is stored across a replicated database (so 2 databases, if one goes down the other steps in) and then also backed up on a 30-day rotation. This is all within Amazon in the Ireland region.
Who has access to the data?	Schools UK staff members have limited access to data. The Schools UK system utilises a granular access policy whereby users can only access areas of the system that they are required to use. Such as the Claims Department may access claims, the New Business Department may only access quotes and basic claim information. Only directors have the ability to generate export reports.

Who is accountable for the data?	Our Schools UK data controller, Mr Peter Riley.
Who is the data shared with?	The main database including all schools and staff information is not shared with anybody outside of the organisation. We do not share or sell data on to any third parties. We do share limited data, such as names of schools, with our wellbeing, HR and OH partners. This is to enable them to confirm our schools as clients and assist with Wellbeing, HR and OH services. Data collected by our partners on these cases is not shared back to Schools UK.
In the event of a data breach, what is the process?	We have various procedures in place to deal with different data breach scenarios. We have an 'instant lock' feature within the system to block and user or group of users, both internally and externally. We have the ability to force all accounts into lockdown or force all to reset passwords. We also store data on secure servers that are regularly updated, monitored and tested.
How will you notify us if a breach occurs?	We have backups of client contact information to ensure that schools would be notified of a data breach by email or phone.
Do you sub-contract to others who may have access or process personal data that belongs to the school?	We have various external service providers for Wellbeing, HR and OH. These only see information on a 'need to know' basis and do not have access to our system. We simply send them a list of school names to confirm our client list to enable them to assist schools. We also have underwriters that require some information for insurance purposes.
Please confirm that you will not allow them to access school data without prior consent from us as Data Controller	Sub-contractors and third party services providers cannot access any data on individuals without prior consent. They do not have the ability to access or view any data within the system.
Please confirm that you have contractual arrangements in place that ensure that they are GDPR compliant, and that deal with the issues of security and breach reporting	We confirm that Schools UK and our systems are GDPR complient.
What processes do you have in place for testing the security of your system?	We have continual security updates and testing procedures in place. These include regular schedule tests as well as testing at every development push. Attempt multiple logins on the applications to see how it responds. Attempt server access.

	Attempt to access a secure endpoint without credentials. Penetration testing. Internal auditing of the system External developer access attempts Subscribe to AWS updates and security announcements
When was this security system last tested and what was the outcome?	The security of the system is tested at least monthly. It is also tested when updates are made on a weekly basis. The outcome was that the system is still secure.
What actions are you taking to ensure compliance with the GDPR?	We have updated out sales website as well as our system to ensure all communication End-to-End is encrypted. This removes the possibility of interception of data during transfer. We have moved our services to a cloud based system, using AWS secure servers.
Please provide details of your Privacy Policy	https://www.SchoolsUK.com/privacy-policy
Data controller information	Schools UK Peter Riley Position: Director data@Schools UK.com

Other information regarding the Schools UK system and GDPR and Data Processing:

All servers are protected by a hardware firewall which means our IP addresses have to be added within the Amazon account to gain access to the servers terminal. The servers terminal is then protected by a 2048-bit key, not a password, which would make it extremely difficult should someone manage to circumvent the firewall. All updates and deployments are also done in this way, our deployment service's IP addresses and unique keys are added to the firewall. The only way to connect to the database server is on the local network internally through the web server.

Passwords are one-way hashed (irreversible encryption) using the updated Blowfish encryption engine, it would be incredibly difficult to crack a good password even if they had the hash which is secure in our database and scrubbed from any output of the data. This also means we cannot retrieve passwords - however passwords are sent by email to the user.

Brute force protection has been added to all login endpoints, so should someone even want to spent the time trying to brute force a password - they will be locked out after 10 tries and timed out for 30 minutes - this removes the ability to say try thousands of passwords a minute and limits them to say several passwords every 10 minutes.

Login sessions are managed in the form of tokens, a user transmits their email address/password over a secure connection once, and if correct they are given back a randomised 64-bit token for all future calls - this expires after a pre-determined amount of time. All data is served over secure SSL.

All files in the system (e.g. absence doctors notes) are stored using the Amazon S3 system also in Ireland, these files are stored using a completely randomised name such as 6862_wf8et.pdf and directory listings are turned off.

Should you have any further questions regarding our data processes or GDPR compliance, please email data@schoolsuk.com