Security Measures

How we protect you

Protecting your data

We are committed to the security of our customers' data and provide multiple layers of protection for the personal information you entrust to the **SPA***platform*.
In the **(well over a) decade** that we have been providing SPA software tools to schools, we have never had a malicious or harmful security breach.

You control access

As a **SPA***platform* customer, you have the flexibility to invite an unlimited number of users into your account to collaborate on your data, but only the people you make 'administrators' will have control over who has access and what they are able to do. Our customer support staff will not access your information unless you invite them to help.

If you would like help adding users, then feel free to contact our support team.

If we are contacted by one of your staff members requesting various staff be added to your account or permissions be changed, in most cases where we have not had previous contact with this person, we will phone the school directly to ensure the legitimacy of the request.

User authentication

We provide users access to the **SPA***platform* software through a login and password. We recommend you ask staff to use complex passwords of at least 14 characters that contain a mixture of upper- & lower-case letters, numbers, and special characters (these are current industry recommendations) as it reduces the risk of your **SPA***platform* account being accessed maliciously and your passwords being compromised.

Data encryption

Data transmitted between you and the **SPA***platform* servers is encrypted using the industry-standard TLS 1.2 protocol, protecting your personal data. Your data is also encrypted when we transfer it between data centres for backup and replication.

Network protection

The **SPA***platform* takes a “defence in depth” approach to protecting our systems and your data. Multiple layers of security controls protect access to and within our environment, including firewalls and network/server segregation. We partner with industry-leading server vendors to leverage their expertise to protect our systems.

Secure data centres

The **SPA***platform* servers are located in Australia within enterprise-grade hosting facilities that employ robust physical security controls to prevent physical access to the servers they house. These controls include 24/7/365 monitoring and surveillance, on-site security staff and regular ongoing security audits. The **SPA***platform* maintains multiple geographically separated data replicas and hosting environments to minimise the risk of data loss or outages.

Security monitoring

The **SPA***platform* server team monitors security systems and conducts regular patch updates to identify and manage threats.

Always there

Best-in-class availability

With a record of 99.97% uptime, the **SPA***platform* delivers best-in-class availability. We use multiple redundancy technologies for our hardware, networks, data centres, and infrastructure. These ensure that if any component fails, the **SPA***platform* will keep on running—with little or no disruption to your service.

Built to perform at scale

The **SPA***platform* has been designed to grow with your school. Our high-performance servers, networks, and infrastructure ensure we can deliver quality service to you and our other users.

Disaster recovery and readiness

The **SPA***platform* performs daily replications between our geographically diverse, protected facilities to ensure your data is available and safely stored. This means that even in the unlikely event an entire hosting facility fails, we can switch over quickly to a backup site to keep the **SPA***platform* running. We transmit data securely, across encrypted links.

Constant updates and innovation

We are constantly enhancing the **SPA***platform*, delivering new features and performance improvements. Updates are delivered frequently, with the majority of them being delivered without interrupting our service or disrupting users.

Phishing and malicious emails

In the **(well over a) decade** that the **SPA***platform* has been available to schools, we have never been involved with a phishing or malicious email hoax. However, it is important that we remind our users of the tricks cyber criminals use to get access to your sensitive information, such as your usernames and passwords, etc.

Phishing and malicious emails may look as though they have come from a trustworthy source, but will attempt to trick you into:

- clicking on a link that will infect your computer with malicious software
- following a link to a fake (but convincing-looking) website that will steal your login details
- opening an attachment that will infect your computer.

Once you are hooked, the cyber-criminal may be able gather sensitive personal or school information that they can use for other attacks. However, you can protect yourself and your school by being aware of these scams, and by knowing what to look for that may help you identify a malicious email:

- Incorrect spelling or grammar: legitimate organisations don’t always get it 100% right, but be suspicious of emails with basic errors.
- The actual linked URL is different from the one displayed—hover your mouse over any links in an email (DON’T CLICK) to see if the actual URL is different.
- The email asks for personal information that they should already have, or information that isn’t relevant to your business with them.
- The email calls for urgent action. For example, “Your **SPA***platform* account will be closed if you don’t respond right away”. If you are not sure and want to check, then contact the company you have a relationship with. Don’t click on the link in the email. If the email says you’ve won a competition you didn’t enter, have a parcel waiting that you didn’t order, or promises huge rewards for your help—on the internet, if it sounds too good to be true, then it probably isn’t true.
- There are changes to how information is usually presented. For example, if an email is addressed to “Dear Sirs” or “Hello” instead of to you by name, the

sending email address looks different or complex, or the content is not what you would usually expect.

These are just a few of the things to watch out for. There’s a lot more information and tips available on the web. But even if there’s nothing specific you can point to, the email may just not feel right. Trust your instincts, and don’t get hooked.

If you suspect you’ve received a phishing or malicious email, and it says it’s from **SPA***platform* or SREAMS or uses our logos, do not click on anything in the email—please report it by forwarding the email to support@sreams.com.au.

Try to avoid a phishing attack by following these rules

If you receive a suspicious email, make sure you:

1. DO NOT CLICK on any link or attachment contained in the email.
2. DO NOT REPLY to the email.
3. Report the email by forwarding it to support@sreams.com.au if it is **SPA***platform*-branded.
4. Delete the email.
5. Update your anti-malware (anti-virus, anti-spyware) software, and run a full scan on your computer.

Security Noticeboard

The **SPA***platform* newsfeed (the home screen when logged into the **SPA***platform*) is where you'll find updates on known phishing and other scams targeting our community, as well as any recommendations on how to protect yourself from them. We'll also post other security related news from the **SPA***platform* on the Noticeboard. If you have questions about security matters, or notice any unusual activity or emails related to the **SPA***platform*, please get in touch with our support team.