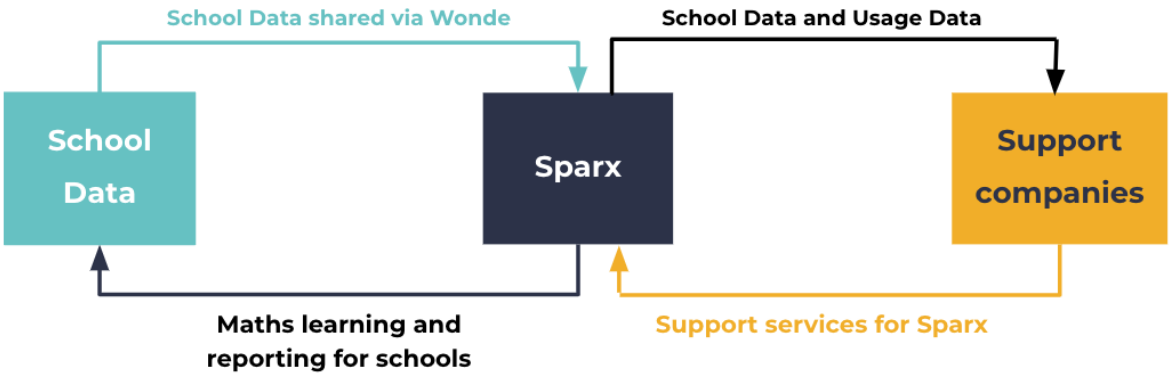
Security Information for Schools

How the Sparx platform works



Security is central to how we deliver Sparx Maths to schools. We have implemented appropriate technical and organisational measures to ensure the personal information shared by schools with us is kept secure.

Schools share personal information about their students, parents, teachers and other school staff with us. We call this **School Data**. We also collect data when Sparx Maths is being used. We call this **Usage Data**.

School Data is securely transferred to us via the Wonde portal. We combine School Data and Usage Data to provide Sparx Maths. School Data and Usage Data is processed by us and our carefully selected third party service providers who support us to deliver Sparx Maths to schools (**support companies**).

- A full list of the support companies engaged by us, including their location, can be found here.
- More information about Wonde's security measures can be found here.

Technical security measures at Sparx

- **Product security**
  - **Encryption practices:** All application data is encrypted at rest as per the default behaviour of Google Cloud Platform (**GCP**) and is transmitted encrypted using https for secure communication. Cryptographic keys are stored securely under carefully restricted access and secrets are rotated periodically.
  - **Network security:** We adopt GCP best practices for network security.
  - **Log-in security:** All passwords are stored securely using industry standard encryption algorithms. Login attempts from a single source are limited to guard against a malicious user trying to guess login details.

    - **Back-ups:** We are responsible for arranging the back-ups of School Data and Usage Data, and managing the archiving process. If there is a loss of School Data for any reason, we will provide recovery services to try to restore the most recent back-up.
- **Internal security**
    - **Device security measures:**
        - Staff work on Macs, Chromebooks and iOS devices which are centrally secured using mobile device management tools to lock down, apply system policies and monitor and enforce patching levels.
        - All can be remotely locked and wiped if necessary.
        - The absence of any Windows devices decreases our device security risk.
        - Local firewalls are implemented on all devices to protect from external threats.
        - All devices password-lock automatically.
    - **Password and authentication policies:**
        - All staff use an enterprise password manager to manage passwords and authentication, with enforced use of a second factor to login.
        - All key tools and services are secured via single sign-on to our authentication tool, and all other tools have complex password policies and multifactor enabled where possible.
        - Strong passwords are used for device logins and master passwords.
    - **In-system policies:**
        - Policies are implemented so that system and data access by staff is limited to that which is necessary to fulfill their role.
        - Where possible all services have staff permissions applied via individual users and security groups, with audit trails kept via our support tool.
        - Access to School Data and Usage Data is tracked and minimised to those who need it and access is time limited where appropriate.
- **Vulnerability detection**
    - **Auditing:** All source code dependencies are automatically scanned for security vulnerabilities by our software development environment. Vulnerabilities are resolved at point of detection and as part of periodic review.
    - **External website security testing:**
        - Rather than traditional 6 monthly / annual penetration testing,, we use web application scanning and “white hat” ethical hacker testing due to the speed that we are developing the product.
        - Daily site vulnerability testing allows us to patch and respond to issues faster.

        - We work with ethical hackers to probe for vulnerabilities in our product in a way that a traditional penetration test or web scan wouldn't be able to detect.
- **Engaging support companies:** We conduct due diligence on our support companies in order to ensure they have good privacy safeguards and security features in place to prevent unauthorised access to the information we send them. **No School Data relating to students (Student Data) is transferred outside the EEA – we will notify schools should there be a change to the international transfer of Student Data.** Please see our Privacy Notice for Schools for further information.
- **Minimisation:** We follow a data minimisation approach and only use the minimum number of data fields to achieve the aims of the processing undertaken on behalf of schools. Wherever possible, identifying personal information is withheld or removed so that anonymised information is used.

Organisational security measures at Sparx

- **Security Team:** We have a Security Team that works to continuously implement, monitor and review security systems and processes.
- **Data Protection Officer:** We are committed to protecting and respecting privacy. We have appointed a Data Protection Officer who advises on, and oversees matters relating to privacy and data security.
- **Organisational policies:** We have a number of policies which provide information and guidance for staff to ensure they maintain the confidentiality of the personal information they work with. The policies detail our security measures and standards, and how staff can positively contribute to ensuring these are met.
- **Training:** Our staff receive security and data protection induction training and regular refresher training. Additionally, all staff can easily access further security and data protection expertise and guidance by approaching the Security Team and Data Protection Officer.
- **Screening, onboarding and offboarding:** Our staff are subject to pre-employment checks. All staff undergo a rigorous induction programme which includes IT security and data protection training. There is an off-boarding process for staff which includes return and decommissioning of IT equipment and removal of access to our systems.
- **Access controls:** As part of implementing our data minimisation approach, we ensure that only our staff and support companies who need access to information are provided with access. System groups and policies are set up to limit and control access to information.
- **Physical security:** Our premises have comprehensive security measures in place and documented disaster recovery plans. Staff have received training and ongoing support for remote working.

If you believe that you have spotted a vulnerability on the Sparx Maths web platform, you can report it at vulnerabilities@sparx.co.uk.