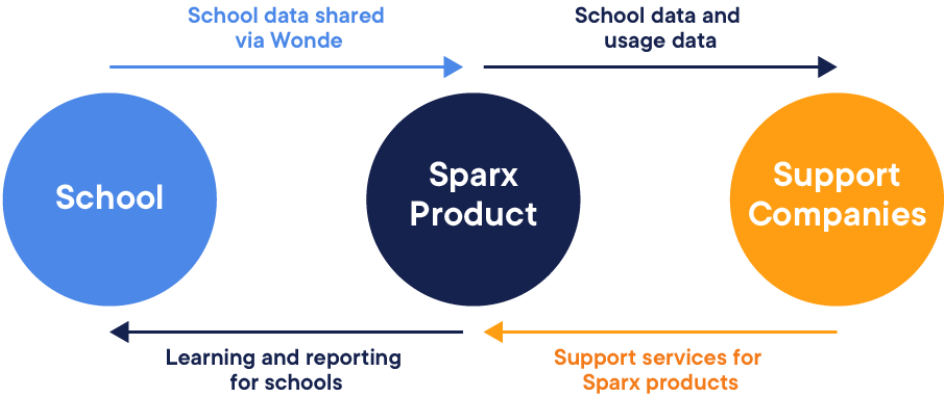
Security Information for Schools (September 2023)

How the Sparx Products work



Security of personal data is central to how we deliver Sparx Maths Homework, Sparx Reader and/or Sparx Science (together referred to as the Sparx Products and each a Sparx Product) to your school. We have implemented appropriate technical and organisational measures to ensure the personal data shared by schools with us is kept secure.

Schools share personal data 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 transferred securely to us via Wonde. We combine school data and usage data to provide the Sparx Product. School data and usage data are processed by us and carefully selected, audited and approved sub-processors who support us to deliver the Sparx Product to you (support companies). A list of our support companies is available here. Information about Wonde's security measures can be found here.

If you believe that you have spotted a vulnerability in the Sparx Product, you can report it at vulnerabilities@sparx.co.uk.

Where we store our data

Sparx uses Google Cloud Platform (GCP) for cloud computing services, including hosting our platform and storing student, teacher and parent personal data. All our user data is stored on GCP servers that are located in the European Economic Area, including back-ups. Our primary storage servers are Belgium, GCP Europe server EUROPE-WEST1. Our backups are hosted under Google's European Multi-regional bucket. This means that Google can choose which of its servers they use but it can never leave the EU. You can read more about GCP servers or 'storage buckets' here.

All application data is encrypted at rest and is transmitted encrypted using https for secure communication. Cryptographic keys are stored securely under carefully restricted access and secrets are rotated periodically.

Technical security measures

Product Security	• Encryption practices: All school data is encrypted at rest.
	• Log-in security:
	  ○ All passwords are stored securely using industry-standard encryption algorithms.
	  ○ Technology is in place to protect against brute force attacks.

	• Secure back-ups:
	  ○ We securely back up school data and usage data.
	  ○ Back-ups are run daily and are fully encrypted.
	• Data deletion:
	  ○ Personal data is securely deleted in line with industry standards in accordance with our retention policy. Deletion logs are maintained.
	• Vulnerability detection:
	  ○ Regular vulnerability assessments exceeding industry standards are undertaken.
	• Penetration Testing:
	  ○ Regular external penetration tests take place using third-party experts.

Internal Security	• Device security:
	  ○ Staff work on devices which are centrally managed and secured using mobile device management tools.
	  ○ All devices have hard disk encryption and automated password locking enforced.
	  ○ Local firewalls are implemented on all corporate laptops.
	  ○ Patch management for corporate laptops exceeds industry standards.
	  ○ We implement an endpoint detection and response solution to maintain device compliance, prevent malware and detect and remediate specific threats.
	• Password and authentication policies:
	  ○ We have implemented an enterprise password manager with enforced multi-factor authentication (MFA).
	  ○ All key tools and services are secured using MFA.
	  ○ Complex passwords are enforced exceeding industry standards..
	• Zero trust:
	  ○ Policies and processes are implemented so that access by staff is appropriately restricted.
	  ○ All key tools and services have staff permissions applied via individual users and security groups with audit trails.
	• Vulnerability detection:
	  ○ Regular vulnerability assessments exceeding industry standards are undertaken.
	  ○ Source code is automatically scanned for security vulnerabilities and remediated where necessary.
	  ○ We aim to patch all known critical and high vulnerabilities within 14 days.

Organisational security measures

- Security Team:
  - We have a dedicated security team that meets regularly to manage security risks and report to the board.
  - A third-party specialist consultant has been retained to advise on information security.

- Data Protection Team: We have a dedicated data protection team that advises on, and oversees privacy matters. They can be contacted at privacy@sparx.co.uk.
- Organisational policies and processes: Policies and processes are in place to maintain the confidentiality of personal data. These policies and processes are reviewed and audited regularly. Risk registers are maintained to ensure that identified risks are being appropriately managed. We have established management processes to ensure that any incidents that arise are appropriately investigated and resolved. We have never had a breach notifiable to the Information Commissioner's Office.
- Training: All staff receive security and data protection training.
- Screening:
    - All staff are subject to pre-employment checks and onboarding training.
    - We have an off-boarding process for staff which includes the return and decommissioning of IT equipment and the removal of access to our systems.
- Physical security: Our premises have security measures in place including CCTV and monitored access.
- Accreditation: Sparx previously held Cyber Essentials Plus. We took the decision not to renew, however, as schools are increasingly recognising security accreditation, we are currently re-certifying.