SIMS

ParentPay

Questions to ask when choosing a supplier

Schools and MATs should find out about their prospective provider's controls, policies and practices. It's important to know how the provider will ensure the safety and security of your data in order to protect your school.

At a glance, the key questions schools should consider asking fall into the following categories:

1 Organisation and Governance

- Who is responsible for information security – is this a dedicated role? At what level?
- Do you have a dedicated team for cyber security? If so, how many people?
- Do you have a cyber insurance policy? What level of coverage does it provide?
- Can you describe your cyber security strategy? What is your cyber security budget?

2 Data management

- Where is your customer data stored, processed or transmitted?
- What is your data retention schedule in terms of customers' personal data?
- Who are your key suppliers and sub-processors?
- Can you share your records of processing as required by GDPR?

3 Network security

- How often are penetration exercises conducted?
- Is there an established patching strategy in place?
- Are controls in place to monitor internet and email access eg spam and content filters?
- Do you have a method of identifying network security vulnerabilities?
- How quickly are critical weaknesses remediated?
- What anti-virus and anti-malware controls are used to protect customers' data?

4 Data encryption

- Is your customer data protected by encryption during transmission?
- Is customer data encrypted at rest? If so, please describe – at what level.
- Are staff laptops encrypted and if so, what methods are used?
- Where are backups stored? And how are these secured?

5 Access controls

- Are access levels granted based on the principle of least privilege?
- Are password criteria for networks, systems and applications sufficiently complex?
- Is MFA enforced for all employees? Are there any systems excluded from this policy?
- How often are the access levels reviewed?
- How is access safely revoked when people leave the business?

6 Incident response

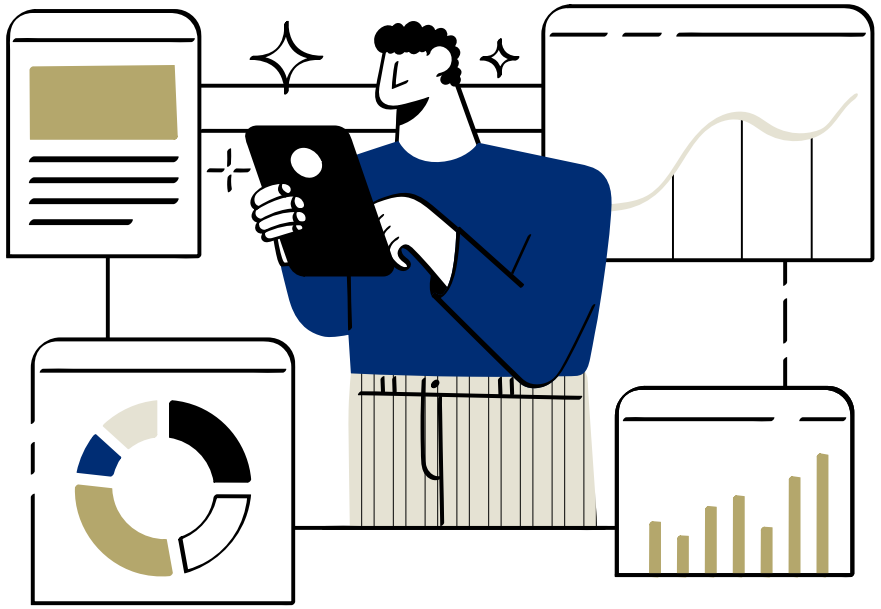
- Do you have a method for identifying and responding to security incidents?
- Do you have a notification process to make customers aware of any relevant breaches?
- When did you last complete a full test if your incident response process?
- Are backup and restore procedures tested on a regular basis?

7 Compliance and data regulation

- Are you fully compliant with GDPR and UK Data Protection Act principles?
- Are you registered with the UK Information Commissioner's Office?
- What relevant certifications do you hold?
- Where can we find your privacy notice and data processing agreements?

The combination of research into a vendor's credentials, and the responses to these questions should provide enough information to help schools select safe suppliers.

However, if you're unhappy with the answers, it might be wise to widen your search.



Not all vendors are equal, and cyber security is too important to be left to chance.