Third-party suppliers for schools:

Questions to ask when choosing your supplier

Department for Education

Use this checklist to learn about a supplier's cyber security understanding and provisions.

Do they have cyber security certifications?

The most common standard expected is Cyber Essentials or Cyber Essentials Plus. Larger or highly critical suppliers may require an ISO 27001 certification.

Notes:

Do they comply with the ICT standards for education settings?

They should be aware of and comply with all the DfE Meeting digital and technology standards.

Notes:

Are they compliant with UK GDPR?

Ask:

- how they process, store, and securely delete sensitive school data
- to see their privacy and data retention policies

Notes:

Third-party suppliers for schools:

Questions to ask when choosing your supplier

Department for Education

Where will our data be hosted, and is it encrypted?

Confirm data is encrypted both “at rest and in transit”. This means:

- protecting sensitive information at all stages
- ensuring data is unreadable to unauthorised parties, whether it is sitting securely in storage or moving across networks

Notes:

How do they control access to your systems?

Check they implement multi-factor authentication for all accounts, and how they make sure staff cannot access data they do not need. Make sure information is not, and cannot be, accessed outside of the UK.

Notes:

How do they vet and train your own employees?

Ask for evidence of their staff background checks and regular cyber security awareness training.

Notes:

Third-party suppliers for schools:

Questions to ask when choosing your supplier

Department for Education

Do they have disaster recovery and business continuity plans that have been tested?

Ask what happens if they suffer a ransomware attack or outage, and how quickly they can restore your services.

Make sure they provide secure, accessible, and frequently tested data backups. Ask to see their incident response plans and check who is accountable for data recovery if there is a breach.

Notes:

How and when will they notify you of a data breach?

The contract should have clear requirements for managing and reporting incidents, and timescales for alerting the school.

Notes:

What is their process for a cyber breach involving your data?

Make sure there are clear instructions on roles and responsibilities.

Notes:

Third-party suppliers for schools:

Questions to ask when choosing your supplier

Department for Education

☐ **Do they outsource any part of this service to third parties or cloud service providers?**

If they use subcontractors, check if they have access to your data. Check they have background checks in place for their own employees and vendors.

Notes:

☐ **What happens to your data if they go out of business?**

Make sure there is a clear plan to securely get your data back.

Notes:

Find out more about choosing a third-party supplier on the Department for Education Cyber Security Hub.

https://cyber-security-hub.education.gov.uk/third-party-suppliers