GDPR Checklist for Suppliers

Questions Schools Need to Ask

1. Are you able to prove your GDPR compliance? What steps have you taken to ensure compliance?
Although there is no GDPR certification in place to prove compliance, suppliers should be able to demonstrate compliance and detail the steps they have taken to be so.

2. What personal data do you process?
They should be able to provide you a list of the data they process and provide detail in a Privacy Policy that includes their purpose for processing and who it will be shared with.

3. Do you have a process for Subject Access Requests?
The supplier should confirm that they do and should let you know who in their organisation should be contacted for this.

4. Does your team have adequate data protection training?
If required, the supplier may have appointed a Data Protection Officer (DPO), who will have undergone training in data protection. The majority of suppliers working with schools will be required to do so if their "core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or large scale processing of special categories of data." (Data Protection Officers, ICO) There should also be company-wide training in place.

5. What is the lawful basis for processing the personal data you hold?
The supplier should let you know the legal basis they have for processing data. They may have more than one and should provide full details of which basis/bases they are processing under in their Privacy Policy.

6. Have you reviewed your consent processes and if so how?
If the supplier is using consent as a lawful basis for processing any data, they should have updated the ways they obtain consent and allow individuals to opt out.

7. Do you have procedures in place to detect, investigate and if necessary, report a breach?
They should confirm that they do and give you details of these procedures.

8. Does your contract and Data Sharing Agreement meet the needs of our school and describe obligations for both supplier (processor) and school (controller) clearly?
This is dependent on the needs of your school, but any GDPR-compliant contract should outline both the school's and the supplier's responsibilities and a Data Sharing Agreement.

9. Will they give you advance warning of any sub-processors?
Suppliers should confirm that they'll let you know if they update the way they process personal data though a sub-processor e.g. MIS/SSO integrations.

10. What measures are in place for increased security?
Processors are required to implement appropriate security measures to protect the personal data they store and process.

11. Have you carried out a Data Protection Impact Assessment?
It's good practice to carry out a DPIA to identify potential data protection risks and to minimise them. However, it's also required if processing data that is likely to result in a high risk to individuals' interests - this will be the case for many suppliers and they most likely should confirm they have carried out a DPIA.

Useful audit resource: GDPRiS - School Data EcoSytstem