****

**Data Processor Checklist**

**Version Control**

|  |
| --- |
| **Scope: Applicable to all Trust Schools** |
| Date to Board: | 10/07/2024 |
| Review date: | Summer Term 2025 |
| Union Consultation Date: | N/A |
| Statutory or non-statutory: | Non-Statutory  |
| Author/Reviewer: | Catherine Cox - TEO |

**Guidance to the Data processor Checklist**

This checklist should be used whenever you are using a third party to deal with personal data on your behalf. You will continue to be responsible for the information, and the third party will be restricted to doing only what you tell them. They will have no right to keep or use the information for any of their own purposes. You will be the Data Controller, and the third party is the Data Processor.

Controllers are required to use only processors providing sufficient guarantees to implement appropriate data protection measures and ensure compliance. Adherence of a processor to an approved code of conduct or approved certification assists in demonstrating that sufficient guarantees exist. We recommend that the Processor’s adherence to an approved code of conduct or approved certification should be recited in the agreement you have with the Processor.

To comply with the law, your agreement with the Processor must:

* Be in writing
* Contain the following information on the processing:
* its subject matter and duration;
* the nature and purpose of the processing;
* the type of personal data;
* the categories of individuals who are the data subjects.
* Expressly state that the Processor can only act on your instructions as the Controller.
* Require the Processor to impose a duty of confidentiality on relevant staff.
* Require the Processor to implement relevant security measures to protect the data. You can specify what those measures are, and what you impose will depend upon the type and sensitivity of the information.
* Require the Processor to seek your prior written permission as Controller to engage a sub-contractor.
* Require the Processor to make all necessary arrangements to ensure that as the Controller you can respect the rights of the individuals under data protection law. As an example, the Processor must be required to make available any personal data should an individual make a Subject Access Request; must be able to delete or rectify data if necessary and must enable data portability where applicable.
* Require the Data Processor to have in place the necessary means of assisting you as the Controller to meet your obligations under data protection law. This includes ensuring security of data, co-operating in relation to your notification of breaches to the Information Commissioner’s Office and data subjects, and with preparation of data protection impact assessments.
* Require the Processor to assist you as the Controller in meeting any obligations imposed by the Information Commissioner’s Office, by allowing access to information, and details of activities and systems if and when required.
* Require the Processor to delete or return the data at the end of the contract. The choice of whether the data is returned or deleted is your decision as the Controller.
* Require the Processor to provide you with all necessary information regarding processing activities to demonstrate compliance – including security measures taken, disclosures made, what has been done to the information plus anything else you need to know as Controller to allow the processing to be audited.
* Provide that any legal requirements that the Processor is subject to which may require the disclosure of the personal data (such as Freedom of Information) should be notified to you as the Controller in advance, where possible.
* Be governed by law of England and Wales

Note: The GDPR refers to the possible development of standard clauses covering the compliance matters listed above. The position should therefore be monitored.

CHECKLIST

☐ Agreement is in writing under law of England and Wales

☐ Names of Processor and Controller details

☐ Details of the processing project, its purpose, subject matter and duration

☐ Processor can only act on instructions of Controller

☐ Duty of confidentiality for Processor’s staff

☐ Processor to implement necessary security measures

☐ Only sub-contract with Controller’s permission

☐ Make arrangements which allow Controller to respect rights of data subjects

☐ Assist the Controller with security and other data protection compliance

☐ Assist the Controller with Information Commissioner requirements

☐ Delete or return data at the end of the contract

☐ Details of processing activities to be made available to Controller

☐ Any legal requirements for disclosure to third party by Processor to be notified