Data Processing Clauses in Contracts

Self-Assessment Checklist

The General Data Protection Regulation (the UK GDPR) now obliges Data Controllers (that is the organisation that sets the purposes of data processing) to have a written contract with their Data Processors (that is the organisation who processes the data on their behalf). Whilst this has been best practice for a number of years Article 28 of the UK GDPR now sets certain criteria that must be included within contracts and service level agreements.

This self-assessment checklist should be used by officers to ensure that proposed contract and service level agreement variations meet the criteria set by the Regulation.

This self-assessment should be signed off, by the appropriate Information Asset Owner or senior manager, prior to the contract or service level agreement being varied.

Contract Name and/or Reference Number:	

Part One – Contract Type	**Instruction**
Did this contract originate from the School? *(School template and terms)*	Do not agree to vary the contract. This contract will be identified as part of corporate approach to varying contracts for the UK GDPR.
Did this contract originate from the supplier/partner? *(Supplier template and terms)*	Continue to Part Two

Part Two - Mandatory Details *The UK GDPR states that the following information must be included in contracts. This information will most commonly be found in a Schedule to the contract rather than in the terms and conditions.*	***Check***
The subject matter and duration of the processing *(What is the contract and how long does it last?)*	
The nature and purpose of the processing *(What is the purpose of the data disclosure?)*	
The type of personal data and categories of data subject *(What data will be disclosed and who is the data subject?)*	

Part Three - Mandatory Terms *The following terms must be included within the Contract*	***Check***
The processor must only act on the written instructions of the controller (unless required by law to act without such instructions).	
The processor must ensure that people processing the data (employees) are subject to a duty of confidence.	
The processor must take appropriate measures to ensure the security of processing.	
the processor must only engage a sub-processor (that is a third party organisation) with the prior consent of the data controller and a written contract.	
The processor must assist the data controller in providing subject access	

and allowing data subjects to exercise their rights under the UK GDPR.	
The processor must assist the data controller in meeting its UK GDPR obligations in relation to the security of processing, the notification of personal data breaches, and data protection impact assessments.	
The processor must delete or return all personal data to the controller as requested at the end of the contract (with an explanation as to method of destruction or return.)	
The processor must submit to audits and inspections, provide the controller with whatever information it needs, and tell the controller immediately if it is asked to do something infringing the UK GDPR or other data protection law of the EU or a member state.	

Part Four – Best Practice *The following should be included within the terms of the contract unless exceptional circumstances dictate otherwise (seek legal advice if this is the case)*	***Check***
State that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the UK GDPR	
Reflect any indemnity that has been agreed.	

Completed by:		**Authorised by:** ***(Information Asset Owner or Manager)***	
Name:		*Name:*	
Job Title:		*Job Title:*	
Date:		*Date:*	