Model Data Processing Clauses for Contracts (Long)

For insertion in all relevant new contracts (i.e. those contracts that involve data processing/personal data) awarded on or after 25 May 2018.

NOTE: The standard definitions highlighted below are not specific to the UK GDPR and therefore may need to be amended to fit within your existing contract definitions.

[STANDARD DEFINITIONS WHICH MAY NEED AMENDING:

Party: means a party to this Agreement and "**Parties**" shall be construed accordingly;

Agreement: means this contract;

Law: means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Provider is bound to comply;

Provider Personnel: means all directors, officers, employees, agents, consultants and contractors of the Provider and/or of any Sub-Contractor engaged in the performance of its obligations under this Agreement;**]**

THE UK GDPR CLAUSE DEFINITIONS:

Controller: has the meaning given in the UK GDPR;

Data Loss Event: means any event that results, or may result, in unauthorised access to Personal Data held by the Provider under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach;

Data Processing Schedule: means Schedule [ ] to this Agreement setting out the scope, nature and purpose of processing by the Provider, the duration of the processing and the types of Personal Data and categories of Data Subject; and

Data Protection Impact Assessment: means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;

Data Protection Legislation: means (i) the UK GDPR, the LED and any applicable national
implementing Laws as amended from time to time; (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy; and (iii) all applicable Law about the processing of personal data and privacy;

Data Protection Officer: has the meaning given in the UK GDPR;

Data Subject: has the meaning given in the UK GDPR;

Data Subject Access Request: means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;

DPA 2018: means the Data Protection Act 2018;

The UK GDPR: means the General Data Protection Regulation (*Regulation (EU) 2016/679*);

LED: means the Law Enforcement Directive (*Directive (EU) 2016/680*);

Personal Data: has the meaning given in the UK GDPR;

Personal Data Breach: has the meaning given in the UK GDPR;

Processor: has the meaning given in the UK GDPR;

Protective Measures: means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it;

Sub-processor: means any third party appointed to process Personal Data on behalf of the Provider related to this Agreement;

NOTE: Party One is the Data Controller and Party Two is the Data Processor. So if the Local Authority was providing a traded service to a school (such as payroll) then the School would be Party One and the Local Authority would be Party Two

[1] DATA PROTECTION

1.1 Both Parties shall comply with all applicable requirements of the Data Protection Legislation. This clause [1] is in addition to, and does not relieve, remove or replace, a Party's obligations under the Data Protection Legislation. Each Party shall bear its own costs in relation to compliance with this clause [1] and the Data Protection Legislation.

1.2 The Parties acknowledge that for the purposes of the Data Protection Legislation, [Party One] is the Controller and [Party Two] is the Processor. The only processing that [Party Two] is authorised to do is listed in the Data Processing Schedule by [Party One] and may not be determined by [Party Two].

1.3 [Party Two] shall notify [Party One] immediately if it considers that any of [Party One]’s instructions infringe the Data Protection Legislation.

1.4 [Party Two] shall provide all reasonable assistance to [Party One] in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of [Party One], include:

(a) a systematic description of the envisaged processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.5 [Party Two] shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

(a) process that Personal Data only in accordance with the Data Processing Schedule, unless [Party Two] is required to do otherwise by Law. If it is so required [Party Two] shall promptly notify [Party One] before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, which have been reviewed and approved by [Party One] as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that:

(i) [Party Two] Personnel do not process Personal Data except in accordance with this Agreement (and in particular the Data Processing Schedule);

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Provider Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with [Party Two]'s duties under this clause [1];

(B) are subject to appropriate confidentiality undertakings with [Party Two] or any Sub-processor;

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by [Party One] or as otherwise permitted by this Agreement; and

(D) have undergone adequate training regarding the use, care, protection and handling of Personal Data;

(d) not transfer Personal Data outside of the EU unless the prior written consent of [Party One] has been obtained and the following conditions are fulfilled:

(i) [Party One] or [Party Two] has provided appropriate safeguards in relation to the transfer (whether in accordance with the UK GDPR Article 46 or LED Article 37) as determined by [Party One];

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) [Party Two] complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist [Party One] in meetings its obligations); and

(iv) [Party Two] complies with any reasonable instructions notified to it in advance by [Party One] with respect to the processing of the Personal Data;

(e) at the written direction of [Party One], delete or return Personal Data (and any copies of it) to [Party One] on termination of the Agreement unless [Party Two] is required by Law to retain the Personal Data.

1.6 Subject to clause [1.7], [Party Two] shall notify [Party One] immediately if it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data:

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

(e) receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

(f) becomes aware of a Data Loss Event.

1.7 [Party Two]'s obligation to notify under clause [1.6] shall include the provision of further information to [Party One] in phases, as details become available.

1.8 Taking into account the nature of the processing, [Party Two] shall provide to [Party One] with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause [1.6] (and insofar as possible within the timescales reasonably required by [Party One]) including by promptly providing:

(a) [Party One] with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by [Party One] to enable [Party One] to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

(c) [Party One], at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by [Party One] following any Data Loss Event; and

(e) assistance as requested by [Party One] with respect to any request from the Information Commissioner's Office, or any consultation by [Party One] with the Information Commissioner's Office.

1.9 [Party Two] shall maintain complete and accurate records and information to demonstrate its compliance with this clause [1]. This requirement does not apply where [Party Two] employs fewer than 250 staff, unless:

(a) [Party One] determines that the processing is not occasional;

(b) [Party One] determines the processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; and

(c) [Party One] determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.10 [Party Two] shall allow for audits of its data processing activity and premises by [Party One] or [Party One]'s designated auditor.

1.11 [Party Two] shall comply with the instructions of [Party One] to enable the audits referred to in clause [1.10] to be carried out and [Party Two] shall provide to [Party One] and/or their designated auditor, all reasonable assistance that they require in connection with any audits, including making available to [Party One] all information necessary to demonstrate compliance with its obligations under this Agreement and the Data Protection Legislation.

1.12 [Party Two] shall designate a data protection officer if required by the Data Protection Legislation.

1.13 Before allowing any Sub-processor to process any Personal Data related to this Agreement, [Party Two] must:

(a) notify [Party One] in writing of the intended Sub-processor and processing;

(b) obtain the written consent of [Party One];

(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause [1] such that they apply to the Sub-processor; and

(d) provide [Party One] with such information regarding the Sub-processor as [Party One] may reasonably require.

1.14 [Party Two] shall remain fully liable for all acts or omissions of any Sub-processor.

1.15 [Party Two] shall indemnify [Party One] for any damage, cost or losses (including legal costs) incurred by [Party One] in connection with any third party claim made or threatened against [Party One] in connection with the loss, unauthorised disclosure or breach of the Data Protection Legislation by [Party Two] or any Sub-processor in relation to any Personal Data which [Party Two] is processing on behalf of [Party One] in connection with this Agreement. This indemnity shall not apply to the extent [Party Two]'s act or omission was as a result of the express instruction of [Party One].

1.16 [Party Two] may, at any time on not less than 30 Working Days' notice, revise this clause [1] by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

1.17 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. [Party One] may on not less than thirty (30) Working Days' notice to [Party Two] amend this Agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

1.17 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The School may on not less than thirty (30) Working Days' notice to the Provider amend this Agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

SCHEDULE [ ] DATA PROCESSING, PERSONAL DATA AND DATA SUBJECT

1. The Provider shall comply with any further written instructions with respect to processing by the School.

2. Any such further instructions shall be incorporated into this Schedule [ ].

Description	Details
Subject matter of the processing	[*This should be a high level, short description of what the processing is about i.e. its subject matter*]
Duration of the processing	[*Clearly set out the duration of the processing including dates*]
Nature and purposes of the processing	[*Please be as specific as possible, but make sure that you cover all intended purposes.* *The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.* *The purpose might include: employment processing, statutory obligation, recruitment assessment etc)*]
Type of Personal Data	[*Examples include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc*]
Categories of Data Subject	[*Examples include: Staff (including volunteers, agents, and temporary workers), customers/clients, suppliers, patients, students/pupils, members of the public, users of a particular website etc*]
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	[*Describe how long the data will be retained for, how it be returned or destroyed*]

Veritau