St Bridgets C.E. Primary School

Third Party Data Processing Agreement

UK GDPR07 V1.0
Effective Date: 31/5/19
Author: Lake Mill Consulting Services

Between:

(1) St Bridgets C.E. Primary School of Main Street, Parton, Whitehaven, Cumbria CA28 6NY (the "Data Controller, Primary Processor or Primary Sub-Processor")

and

(2) [NAME OF THIRD PARTY SUPPLIER / DATA PROCESSOR] of [ADDRESS] (the "Data Processor")

Background

(A) St Bridgets C.E. Primary School uses the services of the Data Processor from time to time to [insert activity].

(B) The Parties have agreed to enter into this Agreement to ensure compliance with the General Data Protection Regulation (UKGDPR) and Data Protection Act (DPA18) in relation to all such processing.

(C) The terms of this Agreement are to apply to all data processing carried out for the Data Controller by the Data Processor and to all personal data held by the Data Processor in relation to all such processing whether such personal data is held at the date of this Agreement or received afterwards.

1. Interpretation

The terms and expressions set out in this agreement shall have the following meanings:

"Act" means the Data Protection Act 2018;

"UK GDPR" means the General Data Protection Regulation;

"Contract" means the agreement between the parties for [insert activity] dated [insert date];

"Data Controller", "Data Processor" and "processing" shall have the meanings given to them in the Act / UK GDPR;

"ICO" means the Information Commissioner's Office;

"Personal data" shall include all data relating to an individual that is processed by the Data Processor on behalf of the Data Controller in accordance with this Agreement.

It is agreed as follows:

2. This Agreement sets out various obligations in relation to the processing of data under the Contract. If there is a conflict between the provisions of the Contract and this Agreement, the provisions of this Agreement shall prevail.

OR

The terms of this Agreement are to apply to all data processing carried out for the Data Controller by the Data Processor and to all personal data held by the Data Processor in relation to all such processing whether such personal data is held at the date of this Agreement or received afterwards. The terms of this Agreement shall supersede any previous arrangement, understanding or agreement between the parties relating to data protection.

3. The Data Processor is to carry out [insert activity] and process personal data received from the Data Controller only on the express instructions of designated contacts at the Data Controller which may be specific instructions or instructions of a general nature as set out in the Contract or as otherwise notified by the Data Controller to the Data Processor during the term of the Contract.

4. The Data Processor shall comply at all times with the Act / UK GDPR and shall not perform its obligations under this Agreement or the Contract in such way as to cause the Data Controller to breach any of its applicable obligations under the Act / UK GDPR.

5. All personal data provided to the Data Processor by the Data Controller or obtained by the Data Processor in the course of its work with the Data Controller is strictly confidential and may not be copied, disclosed or processed in any way without the express authority of the Data Controller.

6. The Data Processor agrees to comply with any reasonable measures required by the Data Controller to ensure that its obligations under this Agreement are satisfactorily performed in accordance with all applicable legislation from time to time in force and any best practice guidance issued by the ICO.

7. Where the Data Processor processes personal data (whether stored in the form of physical or electronic records) on behalf of the Data Controller it shall:

7.1 process the personal data only to the extent, and in such manner, as is necessary in order to comply with its obligations under the Contract OR to the Data Controller or as is required by law or any regulatory body including but not limited to the ICO, Caldicott Guidelines and Information Governance;

7.2 implement appropriate technical and organisational measures and take all steps necessary to protect the personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, and promptly supply details of such measures as requested from the Data Controller;

7.3 in furtherance of its obligations under 7.2 above implement and maintain the security measures set out in Schedule 1 to this agreement;

7.4 if so requested by the Data Controller (and within the timescales required by the Data Controller) supply details of the technical and organisational systems in place to safeguard the security of the personal data held and to prevent unauthorised access;

7.5 on reasonable prior notice, permit persons authorised by the Data Controller to enter into any premises on which personal data provided by the Data Controller to the Data Processor is processed and to inspect the Data Processor's systems to ensure that sufficient security measures are in place;

7.6 notify the Data Controller (within two working days) if it receives:

7.6.1 a request from a data subject to have access to that person's personal data;

or

7.6.2 a complaint or request relating to the Data Controller's obligations under the Act / UK GDPR;

7.7 provide the Data Controller with full co-operation and assistance in relation to any complaint or request made, including by:

7.7.1 providing the Data Controller with full details of the complaint or request;

7.7.2 complying with a data access request within the relevant timescale set out in the Act / UK GDPR and in accordance with the Data Controller's instructions;

7.7.3 providing the Data Controller with any personal data it holds in relation to a data subject (within the timescales required by the Data Controller);

7.7.4 providing the Data Controller with any information requested by the Data Controller;

7.8 not process personal data outside the European Economic Area without the prior written consent of the Data Controller and, where the Data Controller consents to a transfer, to comply with the obligations of a Data Controller under the Eighth Data Protection Principle set out in Schedule 1 of the Act by providing an adequate level of protection to any personal data that is transferred;

7.9 not transfer any personal data provided to it by the Data Controller to any third party without the written consent of the Data Controller and ensure that any third party to which it subcontracts any processing has entered into a written contract with the Data Processor which contains all the obligations that are contained in this Agreement and which permits both the Data Processor and the Data Controller to enforce those obligations.

8. The Data Processor shall transfer all personal data to the Data Controller on the Data Controller's request in the formats, at the times and in compliance with the specifications set out in Schedule 2 OR the requirements notified in writing by the Data Controller to the Data Processor from time to time.

9. The Data Processor shall be liable for and shall indemnify (and keep indemnified) the Data Controller against each and every action, proceeding, liability, cost, claim, loss, expense (including reasonable legal fees and disbursements on a solicitor and client basis and demand incurred by the Data Controller which arise directly or in connection with the Data Processor's data processing activities under this Agreement.

10. The Data Processor agrees that in the event that it is notified by the Data Controller that it is not required to provide any further services to the Data Controller under this Agreement, the Data Processor shall transfer a copy of all information (including personal data) held by it in relation to this Agreement to the Data Controller in a format chosen by the Data Controller and/or, at the Data Controller's request, destroy all such information using a secure method which ensures that it cannot be accessed by any third party and shall issue the Data Controller with a written confirmation of secure disposal.

11. All copyright, database right and other intellectual property rights in any personal data processed under this Agreement (including but not limited to any updates, amendments or adaptations to the personal data by

either the Data Controller or the Data Processor) shall belong to the Data Controller. The Data Processor is licensed to use such data only for the term of and in accordance with this Agreement.

12. The Data Processor accepts the obligations in this Agreement in consideration of the Data Controller continuing to use its services.

This Agreement shall be governed by the laws of the England and Wales and the EU.

SIGNED for and on behalf of St Bridgets C.E. Primary School by:

Print Name: ..... Position: ..... Signature: .....

SIGNED for and on behalf of [NAME OF DATA PROCESSOR] by:

Print Name: ..... Position: ..... Signature: .....

Schedule 1

Security Measures to be Adopted by the Data Processor

1. The Data Processor will ensure that in respect of all personal data it receives from or processes on behalf of the Data Controller it maintains security measures to a standard appropriate to:

1.1 the harm that might result from unlawful or unauthorised processing or accidental loss, damage or destruction of the personal data;

1.2 the nature of the personal data.

2. In particular the Data Processor shall:

2.1 have in place and comply with a security policy which:

2.1.1 defines security needs based on a risk assessment;

2.1.2 allocates responsibility for implementing the policy to a specific individual or members of a team;

2.1.3 is provided to the Data Controller on or before the commencement of this Agreement;

2.1.4 is disseminated to all relevant staff; and

2.1.5 provides a mechanism for feedback and review.

2.2 ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the personal data in accordance with best industry practice;

2.3 prevent unauthorised access to the personal data;

2.4 ensure its storage of personal data conforms with best industry practice such that the media on which personal data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to personal data is strictly monitored and controlled;

2.5 have secure methods in place for the transfer of personal data whether in physical form (for instance, by using couriers rather than post) or electronic form (for instance, by using encryption);

2.6 put password protection on computer systems on which personal data is stored and ensure that only authorised personnel are given details of the password;

2.7 take reasonable steps to ensure the reliability of any employees or other individuals who have access to the personal data;

2.8 ensure that any employees or other individuals required to access the personal data are informed of the confidential nature of the personal data and comply with the obligations set out in this Agreement;

2.9 ensure that none of the employees or other individuals who have access to the personal data publish, disclose or divulge any of the personal data to any third party unless directed in writing to do so by the Data Controller;

2.10 have in place methods for detecting and dealing with breaches of security (including loss, damage or destruction of personal data) including:

2.10.1 the ability to identify which individuals have worked with specific personal data;

2.10.2 having a proper procedure in place for investigating and remedying breaches of the data protection principles contained in the Act; and

2.10.3 notifying the Data Controller as soon as any such security breach occurs.

2.11 have a secure procedure for backing up and storing back-ups separately from originals;

2.12 have a secure method of disposing of unwanted personal data including for back-ups, disks, print outs and redundant equipment.

Notes

Processing to Meet the Requirements of the UK GDPR

Data controllers may only appoint data processors that provide sufficient guarantees to implement appropriate technical and organisational measures to ensure processing meets the requirements of the above legislation. Processors are required to process personal data in accordance with the controller's instructions. This is very broad brush and imposes an indirect obligation to comply with many of the requirements that apply to controllers, albeit at their instruction. It is likely that this general requirement will be made specific in the relevant controller/processor contract and it is in the interest of both controllers and processors to make sure obligations are set out as clearly as possible.

Restrictions on Subcontracting

The UK GDPR gives data controllers a wide degree of control in terms of the ability of the processor to subcontract. In effect, data processors require prior written consent. This can be general but even where general consent has been given, the processor is still required to inform the controller of any new sub-processors, giving the controller time to object.

The lead processor is required to reflect the same contractual obligations it has with the controller in a contract with any sub-processors and remains liable to the controller for the actions or inactions of any sub-processor.

Controller/Processor Contract

Data processor activities must be governed by a binding contract with regard to the controller. There is also scope for a contract to be replaced with Member State or Union law. The binding obligations on the processor must cover the duration, nature and purpose of the processing, the types of data processed and the obligations and rights of the controller. There are a number of specific requirements including that the personal data is processed only on documented instructions from the controller, and requirements to assist the controller in complying with many of its obligations. The data processor has an obligation to tell the controller if it believes an instruction to hand information to the data controller breaches the UK GDPR or any other EU or Member State law.