Managing Suppliers & Third-Party Data Process

‘Working Together to expect the best’

2022

Managing Suppliers & Third-Party Data

Last updated: June 2022
Review Date: March 2023

Version: 2

Document owner: DPO

The Federation of Savile Town CE (C) Infant & Nursery School and Thornhill Lees CE (VC) Infant & Nursery School

Introduction

This process applies to all external suppliers, subcontractors and third parties (herein referred to as 'suppliers') that process data on behalf of The Federation of Savile Town CE (C) Infant & Nursery School and Thornhill Lees CE (VC) Infant & Nursery School**.** This policy details the procedure the school will follow throughout the process of managing those suppliers the school will work with from selection through to completion.

Responsibilities

The School Business Manager in conjunction with the Finance Department and Data Protection Officer (DPO) are responsible for approving the selection of suppliers that process personal data on behalf of the school.

The owners of third-party relationships are responsible for ensuring that all data processing is carried out in line with this procedure.

The IT Manager / Department is responsible for ensuring that adequate technical and other resources are available to support and manage the relationship between the school and said suppliers.

The School Business Manager is responsible for carrying out regular audits of supplier compliance.

Procedure

Any supplier that process personal data on behalf of the school will only be selected if they can provide the technical, physical and organisational security required by the school.

Any suppliers outside of the United Kingdom will only be selected if they meet the same high levels of data compliance set out in the UK General Data Protection Regulations and associated Data Protection Act, 1998.

If the School Business Manager and / or Data Protection Officer consider it necessary, a data security risk assessment will be carried out in the form of a questionnaire (Annex A). This will be dependent on the nature of the personal data being processed or the circumstances of the processing.

Where it is not possible to complete a questionnaire, further compliance checks will be made on the supplier to assess compliance; the School Business Manager and DPO will then make a decision on whether to engage.

In most cases, the school will require a written agreement and confirmation of appropriate security measures from the supplier regarding the processing of personal data prior to partaking in any services. An example data sharing agreement from the Information Commissioners Office (ICO) is provided at Annex B should the school need to draft an agreement.

Any data processing agreement with the supplier will allow the school to conduct regular audits of the security arrangements during the period(s) in which the supplier has access to personal information.

Suppliers will need to request written authorisation from the school if they intend to outsource any part of the data processing service they provide. Any contracts with second-level suppliers or subcontractors will only be approved if they agree to comply with at least the same security and provisions of the primary organisation.

When a supplier contract / agreement is terminated, any personal data held by them, and any subcontractors will be securely destroyed or returned to the school.

A register of all suppliers who process personal data will be retained for school records along with any completed data sharing agreements, questionnaires and related documentation.

In addition to the register, a copy of all supplier privacy notices will be retained on the school system to identify how they intend to process and personal data from the school.

ANNEX A

DRAFT LETTER AND INFORMATION SECURITY QUESTIONNAIRE FOR SUPPLIERS, CONTRACTORS AND THIRD PARTIES

[Insert Supplier Name and Address]

Date:

Dear Sir/Madam,

UK-GDPR Compliance

As a school we are continually working towards ensuring compliance with the UK GDPR and Data Protection Act.

As a supplier, sub-contractor or third-party utilising school data, you need to confirm that you have undertaken a necessary review of your processes and procedures to ensure compliance with the relevant data protection laws. To continue with our commercial relationship, we need written confirmation that the current contract or arrangements will be agreeable and reflect the school's compliance standards.

Please complete the series of questions below and explain how you will comply.

We require the enclosed form to be completed, signed and returned to the School School Business Manager either using the electronic system or by post. We reserve the right to request any additional information from you about your processes and procedures that will enable us secure compliance with the UK-GDPR requirements.

As a public authority we have an obligation to be compliant with UK-GDPR and to demonstrate compliance.

Thank you for your assistance.

Kind regards

[insert school name], School Business Manager

School name: [insert school name]

To comply with our compliance arrangements, please ensure that your Company:

Supplier Requirement	**Confirm consent and process**
Only uses the data we provide or that you access from our organisation in accordance with our instructions.	
Ensure that all parties in your organisation understand that any data they have access to or use which relates to our students or staff is confidential and must not be shared with anyone without our prior agreement.	
Take all steps to keep our data secure, whether it is paper records, emails, digital or electronic. Please note, we reserve the right to ask for evidence and details about how this is done.	
If you subcontract any part of the task, and personal information and data is required by that sub-contractor, you will seek and obtain our consent before proceeding with the transfer of any data.	
On occasion, we may receive a request to release information that we hold about an individual whose data you have used or processed on our behalf. Please confirm that in those situations you will co-operate with us and provide all records about the person within a specified timeframe?	
Should there be a data breach, please confirm that you will notify us as soon as you are aware?	
In the event of a breach please confirm that you will co-operate with us to report, manage and recover data that you have also had access to or use?	
In the event of a data breach, what is the process? Please enclose any relevant procedures.	

That you will delete or return (at our choice) all personal data at the end of the agreement (unless storage is required by your current member state law)	
You will make available to the us all information necessary to demonstrate compliance; allow/contribute to audits (including inspections if necessary)	
Please provide answers to the following	
What processes do you have in place for testing the security of your system?	
When was this security system last tested and what was the outcome?	
What is your organisations strategy for achieving compliance with the UK-GDPR?	
Please provide details of your Data Protection/Information Security/Cyber Security Policy as appropriate.	

I, [insert name] on behalf of [insert company name] confirm that the responses above are accurate and conform to the commercial agreement between [insert school name] and [insert company name].

Signed…….

Dated……...

Role within organisation……...

ANNEX B

DATA PROCESSING AGREEMENT FOR USE WITH SUPPLIERS AND OTHER THIRD PARTIES.

To be completed to represent the processing activities by the DPO and Third Party

DATED_____

(1) The Federation of Savile Town CE (C) Infant & Nursery School and Thornhill Lees CE (VC) Infant & Nursery School

(2) <<Name of Data Processor>>

DATA PROCESSING AGREEMENT

THIS AGREEMENT is made the day of

BETWEEN:

(1) **The Federation of Savile Town CE (C) Infant & Nursery School and Thornhill Lees CE (VC) Infant & Nursery School** whose registered office is at Warren Street, Dewsbury, WF12 9LY and **Slaithwaite Road, Dewsbury, West Yorkshire, WF12 9DL** ("Data Controller") and

(2) <<Name of Data Processor>> **[**a company registered in <<Country of Registration>> under number <<Company Registration Number>> whose registered office is at**] OR [**of**]** <<insert Address>> ("Data Processor")

WHEREAS:

(1) Under a written agreement between the Data Controller and the Data Processor dated <<insert date>> ("the Service Agreement") the Data Processor provides to the Data Controller**] OR [**The Data Controller from time to time engages the Data Processor to provide to the Data Controller**]** the Services described in Schedule 1.

(2) The provision of the Services by the Data Processor involves it in processing the Personal Data described in Schedule 2 on behalf of the Data Controller.

(3) Article 28(3) of the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR") requires an agreement in writing between the Data Controller and any organisation which processes Personal Data on its behalf, governing the processing of that Personal Data.

(4) The Parties have agreed to enter into this Agreement to ensure compliance with the said provisions of the UK GDPR in relation to all processing of the Personal Data by the Data Processor for the Data Controller.

(5) The terms of this Agreement are to apply to all processing of Personal Data 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.

IT IS AGREED as follows:

1. **Definitions and Interpretation**

1.1 In this Agreement, unless the context otherwise requires, the following expressions have the following meanings:

"Data Controller"	shall have the meaning given to the term "controller" in section 6 of the Data Protection Act 2018;
"Data Processor"	shall have the meaning given to the term "processor" in Article 4 of the UK GDPR;

"Data Protection Legislation"	means all applicable legislation in force from time to time in the United Kingdom applicable to data protection and privacy including, but not limited to, the UK GDPR, the Data Protection Act 2018 (and regulations made thereunder), and the Privacy and Electronic Communications Regulations 2003 as amended;
"Data Subject"	shall have the meaning given to the term "data subject" in Article 4 of the UK GDPR;
"EEA"	means the European Economic Area, consisting of all EU Member States plus Iceland, Liechtenstein, and Norway;
"Information Commissioner"	means the Information Commissioner, as defined in Article 4(A3) of the UK GDPR and section 114 of the Data Protection Act 2018;
"Personal Data Breach"	shall have the meaning given to the term "personal data breach" in Article 4 of the UK GDPR;
"Personal Data"	means all such "personal data", as defined in Article 4 of the UK GDPR, as is, or is to be, processed by the Data Processor on behalf of the Data Controller, as described in Schedule 2;
"processing", "process", "processes", "processed"	shall have the meaning given to the term "processing" in Article 4 of the UK GDPR;
["Records"	means written records kept by the Data Processor of all processing activities carried out on behalf of the Data Controller, as set out in sub-Clause 13.2;**]**
"Services"	means those **[**services**]** **AND/OR [**facilities**]** described in Schedule 1 which are provided by the Data Processor to the Data Controller and which the Data Controller uses for the purpose**[**s**]** described in Schedule 1; and
"Term"	means the term of this Agreement, as set out in Clause 17.

1.2 Unless the context otherwise requires, each reference in this Agreement to:

a) "writing", and any cognate expression, includes a reference to any communication effected by electronic or facsimile transmission or similar means;

b) a statute or a provision of a statute is a reference to that statute or provision as amended or re-enacted at the relevant time;

c) "this Agreement" is a reference to this Agreement and each of the Schedules as amended or supplemented at the relevant time;

d) a Schedule is a schedule to this Agreement;

e) a Clause or paragraph is a reference to a Clause of this Agreement (other than the Schedules) or a paragraph of the relevant Schedule; and

f) a "Party" or the "Parties" refer to the parties to this Agreement.

1.3 The headings used in this Agreement are for convenience only and shall have no effect upon the interpretation of this Agreement.

1.4 Words imparting the singular number shall include the plural and vice versa.

1.5 References to any gender shall include any other gender.

1.6 References to persons shall include corporations.

2. Scope and Application of this Agreement

2.1 The provisions of this Agreement shall apply to the processing of the Personal Data described in Schedule 2, 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.

2.2 **[**The provisions of this Agreement shall be deemed to be incorporated into the Service Agreement as if expressly set out in it. Subject to sub-Clause 2.3, definitions and interpretations set out in the Service Agreement shall apply to the interpretation of this Agreement.**]**

2.3 In the event of any conflict or ambiguity between any of the provisions of this Agreement and **[**the Service Agreement**] OR [**any other agreement between the Parties**]**, the provisions of this Agreement shall prevail.

3. Provision of the Services and Processing Personal Data

3.1 Schedule 2 describes the type(s) of Personal Data, the category or categories of Data Subject, the nature of the processing to be carried out, the purpose(s) of the processing, and the duration of the processing.

3.2 Subject to sub-Clause 4.1, the Data Processor is only to carry out the Services, and only to process the Personal Data received from the Data Controller:

a) for the purposes of those Services and not for any other purpose;

b) to the extent and in such a manner as is necessary for those purposes; and

c) strictly in accordance with the express written authorisation and instructions of the Data Controller (which may be specific instructions or instructions of a general nature or as otherwise notified by the Data Controller to the Data Processor).

3.3 The Data Controller shall retain control of the Personal Data at all times and shall remain responsible for its compliance with the Data Protection Legislation including, but not limited to, its collection, holding, and processing of the Personal Data, having in place all necessary and appropriate consents and notices to enable the lawful transfer of the Personal Data to the Data Processor, and with respect to the written instructions given to the Data Processor.

4. The Data Processor's Obligations

4.1 As set out above in Clause 3, the Data Processor shall only process the Personal Data to the extent and in such a manner as is necessary for the purposes of the Services and not for any other purpose. All instructions given

by the Data Controller to the Data Processor shall be made in writing and shall at all times be in compliance with the Data Protection Legislation. The Data Processor shall act only on such written instructions from the Data Controller unless the Data Processor is required by domestic law to do otherwise (as per Article 29 of the UK GDPR) (in which case, the Data Processor shall inform the Data Controller of the legal requirement in question before processing the Personal Data for that purpose unless prohibited from doing so by law).

4.2 The Data Processor shall not process the Personal Data in any manner which does not comply with the provisions of this Agreement or with the Data Protection Legislation. The Data Processor must inform the Data Controller **[**immediately**] OR [**promptly**]** if, in its opinion, any instructions given by the Data Controller do not comply with the Data Protection Legislation.

4.3 The Data Processor shall promptly comply with any written request from the Data Controller requiring the Data Processor to amend, transfer, delete (or otherwise dispose of), or to otherwise process the Personal Data.

4.4 The Data Processor shall promptly comply with any written request from the Data Controller requiring the Data Processor to stop, mitigate, or remedy any unauthorised processing involving the Personal Data.

4.5 The Data Processor shall provide all reasonable assistance **[**(at its own cost)**] OR [**(at the Data Controller's cost)**]** to the Data Controller in complying with its obligations under the Data Protection Legislation including, but not limited to, the protection of Data Subjects' rights, the security of processing, the notification of Personal Data Breaches, the conduct of data protection impact assessments, and in dealings with the Information Commissioner (including, but not limited to, consultations with the Information Commissioner where a data protection impact assessment indicates that there is a high risk which cannot be mitigated).

4.6 For the purposes of sub-Clause 4.5, "all reasonable assistance" shall take account of the nature of the processing carried out by the Data Processor and the information available to the Data Processor.

4.7 In the event that the Data Processor becomes aware of any changes to the Data Protection Legislation that may, in its reasonable interpretation, adversely impact its performance of the Services and the processing of the Personal Data **[**either under the Service Agreement or**]** under this Agreement, the Data Processor shall inform the Data Controller promptly.

5. Confidentiality

5.1 The Data Processor shall maintain the Personal Data in confidence, and in particular, unless the Data Controller has given written consent for the Data Processor to do so, the Data Processor shall not disclose the Personal Data to any third party. The Data Processor shall not process or make any use of any Personal Data supplied to it by the Data Controller otherwise than as necessary and for the purposes of the provision of the Services to the Data Controller.

5.2 Nothing in this Agreement shall prevent the Data Processor from complying with any requirement to disclose or process Personal Data where such disclosure or processing is required by domestic law, court, or regulator (including, but not limited to, the Information Commissioner). In such cases, the Data Processor shall notify the Data Controller of the disclosure or processing requirements prior to disclosure or processing (unless such notification is prohibited by domestic law) in order that the Data Controller may challenge the requirement if it wishes to do so.

5.3 The Data Processor shall ensure that all employees who are to access and/or process any of the Personal Data are informed of its confidential nature and are contractually obliged to keep the Personal Data confidential.

6. Employees [and Data Protection Officer[s]]

6.1 The Data Controller has appointed a data protection officer in accordance with Article 37 of the UK GDPR, whose details are as follows: Matthew Keeffe of Keeffe and Associates Ltd.

6.2 **[**The Data Processor has appointed a data protection officer in accordance with Article 37 of the UK GDPR, whose details are as follows: <<insert name of data protection officer>>, <<insert contact details>>.**]**

6.3 The Data Processor shall ensure that all employees who are to access and/or process any of the Personal Data are given suitable training on the Data Protection Legislation, the Data Processor's obligations under it, their obligations under it, and its application to their work, with particular regard to the processing of the Personal Data under this Agreement.

7. Security of Processing

7.1 The Data Processor shall implement appropriate technical and organisational measures **[**as reviewed and approved by the Data Controller and**] OR [**,**]** as described in Schedule 3, and take all steps necessary to protect the Personal Data against unauthorised or unlawful processing or accidental or unlawful loss, destruction, or damage. The Data Processor shall inform the Data Controller in advance of any changes to such measures.

7.2 The measures implemented by the Data Processor shall be appropriate to the nature of the personal data, to the harm that may result from such unauthorised or unlawful processing or accidental or unlawful loss, destruction, or damage (in particular to the rights and freedoms of Data Subjects) and shall have regard for the state of technological development and the costs of implementation.

7.3 The measures implemented by the Data Processor may include, as appropriate, pseudonymisation and encryption of the Personal Data; the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services; the ability to restore the availability of and access to the Personal Data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing, and evaluating the effectiveness of the technical and organisational measures.

7.4 The Data Processor shall, if so requested by the Data Controller (and within the timescales required by the Data Controller) supply further 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 **[**The Data Processor shall document all technical and organisational measures in writing and shall review them on a <<insert frequency>> basis to ensure that they remain suitable and up to date.**]**

8. Data Subject Rights and Complaints

8.1 The Data Processor shall take appropriate technical and organisational measures and provide all reasonable assistance **[**(at its own cost)**] OR [**(at the Data Controller's cost)**]** to the Data Controller in complying with its obligations

under the Data Protection Legislation with particular regard to the following:

a) the rights of Data Subjects under the Data Protection Legislation including, but not limited to, the right of access (data subject access requests), the right to rectification, the right to erasure, portability rights, the right to object to processing, rights relating to automated processing, and rights to restrict processing; and

b) compliance with notices served on the Data Controller by the Information Commissioner pursuant to the Data Protection Legislation.

8.2 In the event that the Data Processor receives any notice, complaint, or other communication relating to the Personal Data processing or to either Party's compliance with the Data Protection Legislation, it shall notify the Data Controller immediately in writing.

8.3 In the event that the Data Processor receives any request from a Data Subject to exercise any of their rights under the Data Protection Legislation including, but not limited to, a data subject access request, it shall notify the Data Controller **[**immediately**] OR [**without undue delay**]**.

8.4 The Data Processor shall cooperate fully **[**(at its own cost)**] OR [**(at the Data Controller's cost)**]** with the Data Controller and provide all reasonable assistance in responding to any complaint, notice, other communication, or Data Subject request, including by:

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

b) providing the necessary information and assistance in order to comply with a subject access request;

c) providing the Data Controller with any Personal Data it holds in relation to a Data Subject (within the timescales required by the Data Controller); and

d) providing the Data Controller with any other information requested by the Data Controller.

8.5 The Data Processor shall act only on the Data Controller's instructions and shall not disclose any Personal Data to any Data Subject or to any other party except as instructed in writing by the Data Controller, or as required by domestic law.

9. Personal Data Breaches

9.1 The Data Processor shall within 24 hours (and without undue delay) notify the Data Controller in writing if it becomes aware of any form of Personal Data Breach including, but not limited to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Personal Data.

9.2 When the Data Processor becomes aware of a Personal Data Breach, it shall provide the following information to the Data Controller in writing without undue delay:

a) a description of the Personal Data Breach including the category or categories of Personal Data involved, the number (approximate or exact, if known) of Personal Data records involved, and the number (approximate or exact, if known) of Data Subjects involved;

b) the likely consequences of the Personal Data Breach; and

c) a description of the measures it has taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

9.3 In the event of a Personal Data Breach as described above, the Parties shall cooperate with one another to investigate it. The Data Processor shall provide all reasonable assistance to the Data Controller including, but not limited to:

a) assisting the Data Controller with its investigation of the Personal Data Breach;

b) providing and facilitating the Data Controller with access to any relevant facilities, operations, and personnel (including, if applicable, former personnel involved in the Personal Data Breach);

c) making available all records, logs, files, reports, and similar as reasonably required by the Data Controller or as otherwise required by the Data Protection Legislation; and

d) promptly taking all reasonable steps to mitigate the effects of the Personal Data Breach and to minimise any damage caused by it.

9.4 The Data Processor shall use all reasonable endeavours to restore any Personal Data lost, destroyed, damaged, corrupted, or otherwise rendered unusable in the Personal Data Breach as soon as possible after becoming aware of the Personal Data Breach.

9.5 The Data Processor shall not inform any third party of any Personal Data Breach as described above without the express written consent of the Data Controller unless it is required to do so by domestic law.

9.6 The Data Controller shall have the sole right to determine whether or not to notify affected Data Subjects, the Information Commissioner, law enforcement agencies, or other applicable regulators of the Personal Data Breach as required by law or other applicable regulations, or at the Data Controller's discretion, including the form of such notification.

9.7 The Data Controller shall have the sole right to determine whether or not to offer any remedy to Data Subjects affected by the Personal Data Breach, including the form and amount of such remedy.

9.8 Subject to the provisions of Clause 16, the Data Processor shall bear all reasonable costs and expenses incurred by it and shall reimburse the Data Controller for all reasonable costs and expenses incurred by the Data Controller in responding to the Personal Data Breach, including the exercise of any functions or carrying out of any obligations by the Data Controller under any provision of this Clause 9, unless the Personal Data Breach resulted from the Data Controller's express written instructions, negligence, breach of this Agreement, or other act or omission of the Data controller, in which case the Data Controller shall instead bear and shall reimburse the Data Processor with such costs and expenses incurred by it.

10. Personal Data Transfers Outside of the UK or the EEA

The Data Processor (and any subcontractor appointed by it) shall not process or transfer the Personal Data outside of the UK or the EEA.

11. **Appointment of Subcontractors**

11.1 The Data Processor shall not subcontract any of its obligations or rights under this Agreement without the prior written consent of the Data Controller (such consent not to be unreasonably withheld).

11.2 In the event that the Data Processor appoints a subcontractor to process any of the Personal Data (with the specific written consent of the Data Controller on a per-subcontractor basis), the Data Processor shall:

a) enter into a written agreement with each subcontractor, which shall impose upon the subcontractor the same obligations, on substantially the same terms, as are imposed upon the Data Processor by this Agreement, particularly with regard to technical and organisational security measures required to comply with the Data Protection Legislation, which shall permit both the Data Processor and the Data Controller to enforce those obligations, and which shall terminate automatically on the termination of this Agreement for any reason;

b) at the written request of the Data Controller, provide copies of such agreements or, as applicable, the relevant parts thereof;

c) ensure that all subcontractors comply fully with their obligations under the abovementioned agreement and under the Data Protection Legislation; and

d) maintain control over all Personal Data transferred to subcontractors.

11.3 In the event that a subcontractor fails to meet its data protection obligations, the Data Processor shall remain fully liable to the Data Controller for the subcontractor's compliance with its data protection obligations.

11.4 The Data Processor shall be deemed to legally control any and all Personal Data that may be at any time controlled practically by, or be in the possession of, any subcontractor appointed by it under this Clause 11.

12. **Return and/or Deletion or Disposal of Personal Data**

12.1 The Data Processor shall, at the written request of the Data Controller (and at the Data Controller's choice), securely delete (or otherwise dispose of) the Personal Data or return it to the Data Controller in the format(s) reasonably requested by the Data Controller within a reasonable time after the earlier of the following:

a) **[**the end of the provision of the Services; or**]**

OR

a) **[**the termination of the Service Agreement, for any reason; or**]**

b) the processing of that Personal Data by the Data Processor is no longer required for the performance of the Data Processor's obligations under **[**this Agreement**] AND/OR [**the Service Agreement**]**.

12.2 Subject to sub-Clause**[**s**]** 12.3 **[**and 12.4**]**, the Data Processor shall not retain all or any part of the Personal Data after deleting (or otherwise disposing of) or returning it under sub-Clause 12.1.

12.3 If the Data Processor is required to retain copies of all or any part of the Personal Data by law, regulation, government, or other regulatory body, it shall inform the Data Controller of such requirement(s) in writing, including precise details of the Personal Data that it is required to retain, the legal basis for the retention, details

of the duration of the retention, and when the retained Personal Data will be deleted (or otherwise disposed of) once it is no longer required to retain it.

12.4 **[**The Data Processor may retain one copy of the Personal Data for up to <<insert period>> for <<insert purpose(s)>> only.**]**

12.5 Upon the deletion (or disposal) of the Personal Data, the Data Processor shall certify the completion of the same in writing to the Data Controller within <<insert period>> of the deletion (or disposal).

12.6 **[**All Personal Data to be deleted or disposed of under this Agreement shall be deleted or disposed of using the following method(s): <<insert description of method(s)>>.**]**

13. **Information [and Records]**

13.1 The Data Processor shall make available to the Data Controller any and all such information as is reasonably required and necessary to demonstrate the Data Processor's compliance with the Data Protection Legislation and this Agreement.

13.2 **[**The Data Processor shall maintain complete, accurate, and up-to-date written Records of all processing activities carried out by the Data Processor on behalf of the Data Controller which shall include:

a) the name and contact details of the Data Processor and the Data Controller and, where applicable, each Party's representative and data protection officer;

b) the categories of processing carried out by the Data Processor; and

c) a general description of the technical and organisational security measures in place, as referred to in Clause 7.**]**

14. **Audits**

14.1 The Data Processor shall, on **[**at least <<insert period>> days'**] OR [**reasonable**]** prior notice, allow the Data Controller or a third-party auditor appointed by the Data Controller to audit the Data Processor's compliance with its obligations under this Agreement and with the Data Protection Legislation.

14.2 The Data Processor shall provide all necessary assistance **[**(at its own cost)**] OR [**(at the Data Controller's cost)**]** in the conduct of such audits including, but not limited to:

a) access (including physical and remote) to, and copies of, all **[**Records and any other**]** relevant information kept by the Data Processor;

b) access to all of its employees who are to access and/or process any of the Personal Data including, where reasonably necessary, arranging interviews between the Data Controller and such employees; and

c) access to and the inspection of all **[**Records,**]** infrastructure, equipment, software, and other systems used to store and/or process the Personal Data.

14.3 The requirement for the Data Controller to give notice under sub-Clause 14.1 shall not apply if the Data Controller has reason to believe that the Data Processor is in breach of any of its obligations under this Agreement or under the Data Protection Legislation, or if it has reason to believe that a Personal

Data Breach has taken place or is taking place.

14.4 The Data Processor must inform the Data Controller **[**immediately**]** **OR** **[**promptly**]** if, in its opinion, any instructions given by the Data Controller or any third-party auditor appointed by the Data Controller do not comply with the Data Protection Legislation.

15. Warranties

15.1 The Data Controller hereby warrants and represents that the Personal Data and its use with respect to **[**the Services**]** **OR** **[**the Service Agreement**]** and this Agreement shall comply with the Data Protection Legislation in all respects including, but not limited to, its collection, holding, and processing.

15.2 The Data Processor hereby warrants and represents that:

a) the Personal Data shall be processed by the Data Processor (and by any subcontractors appointed under Clause 11) in compliance with the Data Protection Legislation and any and all other relevant laws, regulations, enactments, orders, standards, and other similar instruments;

b) it has no reason to believe that the Data Protection Legislation in any way prevents it from complying with its obligations **[**pertaining to the provision of the Services**]** **OR** **[**under the Service Agreement**]**; and

c) it will implement appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful processing or accidental or unlawful loss, destruction, or damage, as set out in Clause 7 and described in Schedule 3.

16. Liability and Indemnity

16.1 The Data Controller shall be liable for, and shall indemnify (and keep indemnified) the Data Processor in respect of, any and all actions, proceedings, liabilities, costs, claims, losses, expenses (including reasonable legal fees and payments on a solicitor and client basis), or demands, suffered or incurred by, awarded against, or agreed to be paid by, the Data Processor **[**and any subcontractor appointed by the Data Processor under Clause 11**]** arising directly or in connection with:

a) any non-compliance by the Data Controller with the Data Protection Legislation;

b) any Personal Data processing carried out by the Data Processor **[**or any subcontractor appointed by the Data Processor under Clause 11**]** in accordance with instructions given by the Data Controller to the extent that the instructions infringe the Data Protection Legislation; or

c) any breach by the Data Controller of its obligations or warranties under this Agreement;

but not to the extent that the same is or are contributed to by any non-compliance by the Data Processor **[**or any subcontractor appointed by the Data Processor under Clause 11**]** with the Data Protection Legislation or its breach of this Agreement.

16.2 The Data Processor shall be liable for, and shall indemnify (and keep indemnified) the Data Controller in respect of, any and all actions, proceedings,

liabilities, costs, claims, losses, expenses (including reasonable legal fees and payments on a solicitor and client basis), or demands, suffered or incurred by, awarded against, or agreed to be paid by, the Data Controller arising directly or in connection with:

a) any non-compliance by the Data Processor **[**or any subcontractor appointed by the Data Processor under Clause 11**]** with the Data Protection Legislation;

b) any Personal data processing carried out by the Data Processor **[**or any subcontractor appointed by the Data Processor under Clause 11**]** which is not in accordance with instructions given by the Data Controller to the extent that the instructions are in compliance with the Data Protection Legislation; or

c) any breach by the Data Processor of its obligations or warranties under this Agreement;

but not to the extent that the same is or are contributed to by any non-compliance by the Data Controller with the Data Protection Legislation or its breach of this Agreement.

16.3 The Data Controller shall not be entitled to claim back from the Data Processor under sub-Clause 16.2 or on any other basis any sums paid in compensation by the Data Controller in respect of any damage to the extent that the Data Controller is liable to indemnify the Data Processor under sub-Clause 16.1.

16.4 Nothing in this Agreement (and in particular, this Clause 16) shall relieve either Party of, or otherwise affect, the liability of either Party to any Data Subject, or for any other breach of that Party's direct obligations under the Data Protection Legislation. Furthermore, the Data Processor hereby acknowledges that it shall remain subject to the authority of the Information Commissioner and shall co-operate fully therewith, as required, and that failure to comply with its obligations as a data processor under the Data Protection Legislation may render it subject to the fines, penalties, and compensation requirements set out in the Data Protection Legislation.

16.5 Nothing in this Clause 16 shall be deemed to be limited, excluded, or prejudiced by any other provision(s) of this Agreement.

16.6 **[**Any limit of liability set out in the Service Agreement shall not apply to any indemnity or reimbursement provisions set out in this Agreement.**]**

17. Term and Termination

17.1 This Agreement shall come into force on <<insert commencement date>> and shall continue in force for the longer of:

a) **[**The duration of the Services, as set out in Schedule 1; or**]**

OR

a) **[**The period that the Service Agreement remains in effect; or**]**

b) The period that the Data Processor has any of the Personal Data in its possession or control.

17.2 Any provision of this Agreement which, expressly or by implication, is to come into force or remain in force on or after **[**its termination or expiry**] OR [**the termination or expiry of the Service Agreement**]** shall remain in full force and effect.

17.3 In the event that changes to the Data Protection Legislation necessitate the re-negotiation of any part this Agreement, either Party may require such re-negotiation.

18. **Notices**

18.1 All notices under or in connection with this Agreement shall be in writing.

18.2 All notices given to the Data Controller under or in connection with this Agreement must be addressed to: <<insert name, position (e.g. data protection officer), and contact details>>.

18.3 All notices given to the Data Processor under or in connection with this Agreement must be addressed to: <<insert name, position (e.g. data protection officer), and contact details>>.

18.4 Notices shall be deemed to have been duly given:

a) when delivered, if delivered by courier or other messenger (including registered mail) during normal business hours of the recipient; or

b) when sent, if transmitted **[**by facsimile or**]** e-mail **[**and a successful transmission report or return receipt is generated**]**; or

c) on the fifth business day following mailing, if mailed by national ordinary mail, postage prepaid.

In each case notices shall be addressed as indicated above.

19. **Law and Jurisdiction**

19.1 This Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall be governed by, and construed in accordance with, the laws of England and Wales.

19.2 Any dispute, controversy, proceedings or claim between the Parties relating to this Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall fall within the jurisdiction of the courts of England and Wales.

SIGNED for and on behalf of the Data Controller by:

<<Name and Title of person signing for the Data Controller>>

_____

Authorised Signature

Date: _____

SIGNED for and on behalf of the Data Processor by:

<<Name and Title of person signing for the Data Processor>>

_____

Authorised Signature

Date: _____

SCHEDULE 1

Services

<<Insert a detailed description of the Services provided by the Data Processor (under the Service Agreement, where relevant)>>.

SCHEDULE 2

Personal Data

Type of Personal Data	Category of Data Subject	Nature of Processing Carried Out	Purpose(s) of Processing	Duration of Processing

SCHEDULE 3

Technical and Organisational Data Protection Measures

The following are the technical and organisational data protection measures referred to in Clause 7:

1. The Data Processor shall 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; and

   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:

      a) defines security needs based on a risk assessment;

      b) allocates responsibility for implementing the policy to a specific individual **[**(such as the Data Processor's data protection officer)**]** or personnel;

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

      d) is disseminated to all relevant staff; and

      e) 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 ensure that all hardware and software used in the processing of the Personal Data is properly maintained, including but not limited to, the installation of all applicable software updates;

   2.4 prevent unauthorised access to the Personal Data;

   2.5 protect the Personal Data using <<insert type of encryption>> encryption;

   2.6 protect the Personal Data using pseudonymisation, where it is practical to do so;

   2.7 ensure that 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;

   2.8 have secure methods in place for the transfer of Personal Data whether in physical form (for example, by using couriers rather than post) or electronic form (for example, by using <<insert type of encryption>> encryption);

   2.9 password protect all computers and other devices on which Personal Data is stored, ensuring that all passwords are secure (<<describe requirements, e.g. upper and lower-case letters, special characters etc.>>), and that passwords are not shared under any circumstances;

   2.10 **[**not allow the storage of the Personal Data on any mobile devices such as

laptops or tablets unless such devices are kept on its premises at all times;**]**

2.11 take reasonable steps to ensure the reliability of personnel who have access to the Personal Data;

2.12 ensure that all employees who are to access and/or process any of the Personal Data are given suitable training on the Data Protection Legislation, the Data Processor's obligations under it, their obligations under it, and its application to their work, with particular regard to the processing of the Personal Data under this Agreement;

2.13 have in place methods for detecting and dealing with breaches of security (including loss, damage, or destruction of Personal Data) including:

2.13.1 the ability to identify which individuals have worked with specific Personal Data;

2.13.2 having a proper procedure in place for investigating and remedying breaches of the Data Protection Legislation; and

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

2.14 have a secure procedure for backing up all electronic Personal Data and storing back-ups separately from originals;

2.15 have a secure method of disposal of unwanted Personal Data including for back-ups, disks, print-outs, and redundant equipment; **[**and**]**

2.16 **[**<<insert additional specific details as required>>; and**]**

2.17 adopt such organisational, operational, and technological processes and procedures as are required to comply with the requirements of ISO/IEC 27001:2013, as appropriate to the Services provided to the Data Controller.