Data Protection Act 1998
Data Processing Agreement

Telford & Wrekin Council & [3rd Party Supplier]

WHEREAS:-

A. The Data Controller and the Data Processor (taking the meanings accorded in Section B 2), have entered into an Agreement to secure the provision and processing of personal and sensitive personal data (hereinafter referred to as the 'data') already identified in **Appendix 1** of this Agreement solely for the purpose of processing [insert purpose]. The data sets will be directly provided by [insert details] via [insert details]. The Data Processor's data centre is [insert details].

The Data Processor will process authorised data sets (as per Appendix 1), solely for the purpose of [insert details], as shown in Schedule B, and in accordance with the obligations of the Data Processor, as shown in Schedule C, in order to support their contractual obligations.

The Data Processor will ensure all of their staff and any sub-contracted staff have undertaken and continue to receive relevant training around data protection and information security.

B. IT IS HEREBY AGREED BETWEEN THE PARTIES IN SCHEDULE A TO THIS AGREEMENT AS FOLLOWS:-

1. Agreement

Clearly defined processing requirements of personal and sensitive personal data between the Data Controller ("Telford & Wrekin Council") and the Data Processor ("[insert details]"), whereby the Data Processor provides [insert details] for the purposes referred to in Schedule B, subject to the warranties and obligations hereinafter contained.

2. Definitions & Interpretations

a) Data Controller – means Telford & Wrekin Council as the organisation who determines the purposes of which the personal data is to be processed;
b) Data Processor – means [insert supplier] as the organisation who will process the information on behalf of the Data Controller
c) Data Subject – means an individual who is the subject of personal data
d) Personal Data – means data that relates to a living individual who can be identified: from the data; or from data or other information that is in the possession of or is likely to come into the possession of the Data Controller
e) Processing - means obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data including: organisation, adaptation or alteration; retrieval, consultation or use; disclosure by transmission, dissemination or otherwise making available; or alignment, combination, blocking, erasure or destruction of the information or data.

3. Warranty and Obligations of Data Processor

a) The Data Processor warrants that it has the necessary legal authority in the United Kingdom where it is established for the purpose of controlling the processing of the data and to use it for the purpose(s) set out herein, and to give warranties and fulfil the undertakings set out herein.

b) The Data Processor will process the data exclusively for purposes and in accordance with the means of processing listed in Schedule B to the exclusion of any other purposes or means of processing.

c) The Data Processor will not enter into any arrangement to process the data outside the United Kingdom without the written permission of Data Controller.

d) The Data Processor has in place security programs and procedures appropriate to the risks presented by the processing, to ensure that unauthorised persons will not have access to the data and that any persons it authorises to have access to the data will be bound by contract or otherwise to respect and maintain the confidentiality and security of the data.

e) The Data Processor warrants that it will comply with the obligations set out in Schedule C and apply them to the processing of the data originally provided or subsequently amended.

4. Applicable Law

The parties to this Agreement shall be subject to English law and specifically the Data Protection Act 1998 in respect of such processing as is governed by this Agreement.

5. Rights of Data Subjects

The obligations of the Data Processor set out in Schedule C are conferred as third party rights on those data subjects, in respect of whom data is accessed for processing under the terms of this Agreement. Therefore, this processing may be the subject of proceedings under the appropriate legal enactments in the Member State in which the Data Processor is established, in respect of the processing of accessed data that is the subject of this Agreement.

6. Suspension of Contract

This agreement can be suspended for 45 working days, if security has been seriously breached. This should be detailed in writing and be evidenced by the Data Processor to the Data Controller. Any suspension will be subject to a risk assessment and a resolution meeting between nominated representatives of the Data Processor and the Data Controller being held. This meeting will take place within 14 working days of the identification of any breach. The suspension may be lifted when the cause of the breach has been satisfactorily investigated and appropriate measures have been taken to address the situation.

7. Indemnity

Each party will keep the other indemnified against all reasonable costs, expenses and claims arising out of any breach of this Agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending party, employees, agents or any other person within the control of the offending partner of any data obtained in connection with this Agreement.

The Data Processor will indemnify the Data Controller against all claims, costs and fines that may arise in connection with data breaches which are the result of the failure of [insert supplier name], its employees, agents or sub-contractors to properly perform their functions.

8. Consequences of Termination of the Contract

If either party terminates the Agreement relating to the accessing of data and its subsequent processing, the Data Processor shall immediately (within 7 days) securely return/transfer, if requested to do so by the Data Controller, all data provided under this Agreement, in its possession or control, and certify in writing to the Data Controller that it has done so, unless this is prohibited by the national law or regulator of the country in which the Data Processor processes the data. Where this is the case, to the extent allowed under such requirements, the data will be kept confidential and will no longer be processed.

SCHEDULES

SCHEDULE A
Data Controller:

Telford & Wrekin Council,
Civic Offices
Coach Central
Telford
TF3 4LF
United Kingdom

Data Protection Act Registration Number: **Z5142391**

Name	Title	Description of Role	Contact Details

And Data Processor:

[Insert supplier name and address]

Registration Number**: [insert supplier ICO registration number]**

Name	Title	Description of Role	Contact Details

SCHEDULE B

Purpose of Processing the Personal Data:

[insert supplier name] ("Data Processor") has been contracted by Telford & Wrekin Council ("Data Controller") to provide [insert service details] for the sole purpose of [insert purpose].

Both personal and sensitive personal data sets are to be processed and the conditions within the Data Protection Act 1998 that support this are:

Schedule 2 (1) – consent of the data subject
Schedule 3 (1) – explicit consent of the data subject.

The data sets, (already identified above in Appendix 1 of this Agreement), will be used solely to [insert service details].

DURATION, REVIEW AND TERMINATION

This Agreement is effective from the signatory date below until the end of the contract period, which is DATE TO BE CONFIRMED

SIGNATORIES:

This Agreement was executed on INSERT DATE WHEN SIGNED.

_____ Date: _____

_____ Date: _____

_____ Date: _____

SCHEDULE C

Obligations of the Data Processor

1. The Data Processor will make such arrangements as are necessary to ensure it has fulfilled, and will continue to fulfil to comply with the requirements of the Data Protection Act 1998 including the warranties set out in Section B.3 of this agreement.

2. Unless there is specific provision elsewhere in this Agreement, the Data Processor shall process the data exclusively for the purposes outlined in Schedule B and shall not disclose, either free of charge or in return for payment, the data to any other legal or natural person, including when there is a legal obligation, a regulatory obligation or where the Data Processor is responding to a request from a regulatory body, in which case the Data Controller must, where this is permitted by such law, be informed in order to establish consent or grounds for non-disclosure, prior to such disclosure.

3. The Data Processor shall, as far as is practicable, notify the Data Controller of any measures to which it is subject that will have an impact on the access and processing of data made under the Agreement.

4. Where the nature of the data being processed warrants it, the Data Controller reserves the right to demand that an enhanced Criminal Records Bureau check of the appropriate level is undertaken on any staff that will have access to the data and confirm (within 7 days) whether such checks have identified any relevant convictions, cautions or other information that may warrant concern.

5. The Data Processor will not disclose or transfer the personal and sensitive personal data to a third party except with the express authority of the Data Controller.

6. The Data Processor must identify to the Data Controller their Data Protection Officer or other person responsible for compliance with data protection legislation.

7. The Data Processor must have a documented data protection policy in place and shall if requested provide a copy to the Data Controller.

8. If so requested by the Data Controller, the Data Processor must provide evidence of measures taken with regard to staff reliability, staff training, data access restrictions and disciplinary procedures.

9. No further use may be made of the data without the written consent of the Data Controller or as specified in this Agreement. No further use shall be made of any depersonalised data, based on the data supplied without the prior written authority of the Data Controller.

10. The Data Processor must not copy, store, print, transmit or produce in any other format (hard or soft) copies of the data that it is authorised to process.

11. Authorised persons of the Data Processor may only process the data by secure means, including encryption of portable, mobile devices or any other processing equipment that may be vulnerable, in order to prevent unauthorised access or disclosure.

12. Should the Data Controller be required to comply with a request for access to information by a data subject, the Data Processor will assist the Data Controller by providing such

information to the Data Controller and supply any copies of the data in its present format within stated timescales. If any of the processing carried out by the Data Processor consists of decisions taken automatically, full details of the logic will be provided to the Data Controller on commencement of the Agreement, except where these details would constitute a trade secret. The Data Processor must make provision for automated decisions to be taken in a non-automated manner, if such a request is made by a data subject.

13. Hard and soft copy data must be protected by adequate technical and organisational security controls. Any equipment or device (portable or otherwise) used for processing the data electronically must be encrypted and protected by physical and technical controls to prevent unauthorised disclosure, theft or corruption. PCs/laptops (or similar) and any storage devices used (including 'cloud' storage facilities), must always be handled in a secure manner. Hard copy data must be kept secure to also prevent unauthorised disclosure, theft or corruption (e.g. locked in secure cabinets when it is not being used, not kept with portable devices).

14. As data may only be made available to authorised persons, care must be taken not to allow any unauthorised person to see it as hard or soft copy, in temporary or permanent stored form or hear its content discussed in a conversation.

15. Adequate protection must be put in place to ensure any electronic data processed on behalf of the Data Controller does not become infected, eg by malicious code, virus.

16. The Data Processor will provide data subjects with a secure means of inputting and amending personal and sensitive personal data.

17. No connection may be made from third party equipment holding the data electronically to any other system, except for a secure connection to the Data Processor's own network, unless adequate provisions are made and approved prior to implementation by the Data Controller, to prevent access to the data by unauthorised persons.

18. No modem or similar device shall connect the equipment holding electronic data to a live telephone line or other type of network connection except as required for the purposes and connections allowed above.

19. The Data Controller reserves the right to inspect any equipment or premises used to carry out the processes and procedures of which this Agreement is the subject. The Data Controller reserves the right to screen any employees of the Data Processor to the extent allowed by law. The Data Controller will provide 14 days' notice of the requirement to undertake such inspections or requirement for screening.

20. The Data Processor will provide the data subject with the same rights of active 'opt in' to receive direct marketing (as per PEC Regulations 2003), correction, blocking, suppression or deletion available to such an individual in accordance with the law, which is applicable to the Data Processor.

21. The Data Processor shall, where necessary, maintain the accuracy and integrity of the data and keep it up to date. The Data Processor shall comply with all instructions from the Data Controller to rectify, delete and update any data and shall confirm to the Data Controller within 14 days that it has done so.

22. The Data Processor will provide data subjects with a complaints handling process.

23. The Data Processor will ensure any actual breaches of physical or technological security that may or has impacted confidentiality, integrity or availability of the Data Controller’s data are immediately reported to the Data Controller’s IT Security Manager.

24. The Data Processor will ensure any actual breaches of the Data Protection Act and or the terms and conditions of this Agreement that may or has impacted the Data Controller’s compliance with data protection legislation are immediately reported to the Data Controller's Information Governance Manager.

Schedule D : Freedom of Information Act 2000

1. The Data Processor acknowledges that the Data Controller has legal responsibilities to make information available under the Freedom of Information Act 2000.

2. The Data Processor shall be given reasonable assistance to the Data Controller to comply with the Act.

3. In particular, the Data Processor shall supply all such information and records (together with reasonable assistance to locate the same) which are needed by the Data Controller to comply with its obligations under the Act.

4. The Data Processor acknowledges that the Data Controller shall have the discretion to disclose any information which is the subject to the contract with the Data Processor to any person who makes a request under the Act and which in the opinion of the Data Controller it has to disclose to discharges its responsibilities under the Act.

5. When exercising its rights under the Act the Data Controller shall consult with the Data Processor and may take account of any reasonable suggestions made by it.

6. The Data Controller shall not be responsible for any loss damage harm or detriment however caused arising from disclosure of information relating to this contract.

SCHEDULE D

[insert nominated officer details for Telford & Wrekin Council]

[insert nominated details for Data Processor]

will each hold a copy of the signed Agreement on behalf of the respective Parties to this Agreement.

APPENDIX 1

Data Sets to be covered by this Agreement

[insert details of data that will be covered]

e.g.

Parent(s) First and Last Name
Address
Post Code
Employee Number
National Insurance Number
Gender
Date of Birth
Email Address
Daytime Telephone Number
Alternative Telephone Number

Child(s) First Name
Child(s) Last Name
Relationship to the Child
Date of Birth
Disability Status
Gender

Type of Childcare (eg Nursery, childminder, nanny)
Care Provider's Name
Care Provider's Bank Account Details
Postcode
Ofsted Number