**Data Processing Agreement**

Date:

PARTIES

1. University of the West of England, Bristol whose address is Coldharbour Lane, Bristol, BS16 1QY (the "Data Controller”) and
2. **Party B** whose address is [DP address] (the "Data Processor”)

BACKGROUND

1. The Data Controller wishes the Data Processor to carry out the work detailed in Appendix 1 (the "Services”);
2. Both parties agree that they have obligations under the Data Protection Legislation (as defined in clause 25.1 );
3. This Agreement records the obligations of both parties.

AGREED TERMS

In providing the Services, the Data Processor shall process Personal Data (as defined below) on behalf of the Data Controller. The type of Personal Data to be processed, and the categories of Data Subjects are as follows:

|  |  |
| --- | --- |
| *Subject matter of processing* (description of service/goods provided by supplier e.g. cloud based learning support tool) |  |
| *Duration of processing* (how long will data be processed for e.g. duration of contract) |  |
| *Purpose of processing* (brief description of how and why personal data is processed e.g. e-mail addresses processed to verify users of software solution) |  |
| *Type of Personal Data* (types of personal data being processed e.g. names, email addresses) |  |
| *Categories of Data Subjects* (whose personal data is being processed e.g. students or staff) |  |

Specifically, the Data Processor shall:

1. Not act in any way so as to cause the Data Controller to breach of any of its obligations under the Data Protection Legislation;
2. Process Personal Data only in accordance with the written instructions of the Data Controller;
3. Process the Personal Data only to the extent, and in such manner, as is necessary for the provision of the Services or as is required by the Data Protection Legislation, or any other applicable law (and immediately inform the Data Controller if it believes any instruction or processing is likely to breach such law) or any regulatory body ;
4. Implement appropriate technological and organisational measures to protect against accidental loss, destruction, damage, alteration or disclosure of any Personal Data. Such measures shall be appropriate to the loss which might result from any unauthorised or unlawful processing, accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected;
5. Take reasonable steps to ensure the reliability of any employees, workers, agents or sub-processors or contractors who have access to the Personal Data;
6. Ensure that any employees, workers or contractors authorised to process the Personal Data are informed of the confidential nature of the Personal Data and comply with the obligations set out in this Agreement;
7. Ensure that the Personal Data is not made available by default to all employees, workers or contractors of the Data Processor or any sub-contractor and only to such individuals as are strictly required in order to meet the obligations under this Agreement have access to the Personal Data;
8. Ensure that all Personal Data is treated as confidential information and is not published, disclosed or divulged to any third party by the Data Processor or any of its employees, workers or contractors, unless directed in writing to do so by the Data Controller;
9. Notify the Data Controller in writing and by email (as soon as possible and always within five working days) if the Data Processor or any of its employees, workers or contractors receives or becomes aware of:
   1. a request from a Data Subject to have access to that person’s Personal Data or otherwise exercise that person’s data subject rights;
   2. a complaint or request relating to the Data Controller’s obligations under the Data Protection Legislation;
10. Co-operate fully with the Data Controller in relation to any complaint or request made by any Data Subject, regulatory body, supervisory authority and/or court of competent jurisdiction, including by promptly (and in any event within the timescales required by the Data Controller):
    1. providing the Data Controller with full details of any complaint or request that it receives directly;
    2. providing reasonable assistance to the Data Controller in dealing with or responding to any request or any complaint;
    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 under the Data Protection Legislation); and
    4. providing the Data Controller with any information (including any information required to demonstrate compliance with the Data Protection Legislation) required by the Data Controller to respond properly to the request or complaint.
11. Permit the Data Controller’s representatives (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit its data processing activities (and/or those of its permitted agents, subsidiaries and sub-processors) and comply with all reasonable requests or directions by the Data Controller to enable the Data Controller to verify and/or procure that the Data Processor is in full compliance with its obligations under this Agreement;
12. Not process Personal Data outside the United Kingdom or European Economic Area (which for the avoidance of doubt includes storage in any cloud or other such facility which is controlled, regulated and/or hosted outside the UK or EEA) without the prior written consent of the Data Controller and, where the Data Controller consents to such transfer, to comply with:
    1. the obligations of the Data Controller under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
    2. any reasonable instructions notified to it by the Data Controller;
13. At the Data Controller's option, return or securely delete all Personal Data (including any copies) from all systems of the Data Processor (i) after the use of the Personal Data for the Services (ii) following termination of this Agreement or (iii) in any circumstance where the Data Controller is required to do so by Data Protection Legislation and provide written confirmation of this to the Data Controller. Where instructed, the Data Processor must return all Personal Data to the Data Controller;
14. Co-operate fully if the Data Controller serves an information notice on the Data Processor requiring the Data Processor within such time and as required by the information notice, to provide the Data Controller with such information as the Data Controller may reasonably require relating to compliance by the Data Processor with the Data Processor’s obligations under this Agreement in connection with the processing of Personal Data;
15. Notify the Data Controller immediately if the Data Processor or any of its employees, workers agents, sub-processors are requested to do any act which would infringe the Data Protection Legislation;
16. Where the Data Processor wishes to appoint a sub-processor to assist it in providing the

Services and such assistance includes the processing of Personal Data on behalf of the Data

Controller, then the Data Processor must obtain the Data Controller’s prior written consent

(which may be withheld in the Data Controller's absolute discretion) to such appointment. It is

a condition of the Data Controller's consent that the Data Processor ensures the sub-processor

enters into written terms which are substantially the same and no less protective of the

Personal Data as contained in this Agreement. The Data Processor shall remain fully liable to

the Data Controller for the performance of the sub-processor's obligations;

1. Promptly (and in any case within 48 hours) notify the Data Controller in writing (providing full details) if any of the Personal Data has been lost, destroyed, damaged, corrupted or accessed by or disclosed to unauthorised third parties or if it suspects or has reason to believe any the Personal Data may have been lost, destroyed, damaged, corrupted or accessed by or disclosed to unauthorised third parties;
2. Not use any new technologies in the provision of the Services which could, when taking into account the nature, scope, context and purpose of the processing to be carried out as part of the relevant Services, result in a high risk for the rights and freedoms of individuals under the Data Protection Legislation or to the security of the Personal Data, save where:
   1. the Data Processor has notified the Data Controller in advance and the Data Controller, with the assistance of the Data Processor, has had a reasonable opportunity to carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Data; and
   2. following such assessment, the Data Controller has provided its written approval to the Data Processor of the envisaged processing;
3. Be liable for and shall fully indemnify the Data Controller (and keep the Data Controller indemnified) against each and every action, proceeding, liability, cost, claim, loss, fine, penalty, expense (including reasonable legal fees and disbursements) and demands incurred by the Data Controller which arise directly or in connection with the Data Processor’s processing activities under this Agreement, including without limitation those arising out of any third party demand, claim or action, or any breach of contract, negligence, fraud, wilful misconduct, breach of statutory duty or non-compliance with any part of the Data Protection Legislation by the Data Processor or its employees, workers, agents, or sub-processors.
4. In addition to the indemnity to the Data Controller above, the Data Processor is hereby notified and acknowledges that under the United Kingdom General Data Protection Regulation, Data Processors may be held directly liable by the Information Commissioner’s Office ("ICO") for any breaches of the Data Protection Legislation by the Data Processor. This may lead to fines being brought directly against the Data Processor by the ICO for breaches of the Data Protection Legislation. In addition, Data Subjects who have been harmed by the improper transfer, storage or disclosure of their Personal Data will be entitled to make direct claims against Data Processors for any breach of their rights under the Data Protection Legislation.

The parties agree:

1. No term of this Agreement shall be enforceable under the Contracts (Rights of Third Parties) Act 1999 by any third party, but this does not affect any right or remedy of a third party which exists or is available apart from under that Act;
2. Notices, including any notification to the University of the West of England, Bristol under Clause 9 above shall be made in writing and delivered by recorded mail to the Assistant Vice-Chancellor for Data Protection, Privacy and Complaints, University of the West of England Bristol, Frenchay Campus, Coldharbour Lane, Bristol, BS16 1QY with an email copy to [VCOExecSupport@UWE.ac.uk](mailto:VCOExecSupport@UWE.ac.uk) and the University’s Data Protection Officer [dataprotection@uwe.ac.uk](mailto:dataprotection@uwe.ac.uk);
3. This Agreement constitutes the entire agreement and understanding between the parties in respect of the matters dealt with in it and supersedes, cancels or nullifies any previous agreement between the parties in relation to such matters;
4. This Agreement shall be governed by and construed in accordance with the law of England and Wales. Each of the parties irrevocably submits for all purposes in connection with this Agreement to the exclusive jurisdiction of the courts of England and Wales;
5. In this Agreement:
   1. “Data Protection Legislation” means any legislation and/or regulation implementing or made pursuant to them including but not limited to the Data Protection Act 2018 (‘DPA 2018’), or which amends, replaces, re-enacts or consolidates any of them (including but not limited to the UK General Data Protection Regulation as amended by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019), and including, where applicable, the guidance and codes of practice issued by the supervisory authorities (including the Information Commissioner’s Office); and
   2. the terms "Data Processor", "Data Controller", ”sub-processor” "process" and "Data Subject" shall have any meaning given to them in the Data Protection Legislation; and
   3. "Personal Data" means personal data (as defined in the Data Protection Legislation) provided by or collected on behalf of the Data Controller.

Signed by authorised representatives for each of the Parties:

|  |  |
| --- | --- |
| **University of the West of England, Bristol**  **(Controller)** | **{Insert name of Data Processor]**  **(Processor)** |
| **Signature …………………………………………………** | **Signature ……………………………………………………** |
| Name: **……………………………………………………** | Name: **………………………………………………………** |
|  |  |
| Position: **……………………………………………….…** | Position: **……………………………………………….…** |
|  |  |
| Date: **………………………………………………………** | Date: **……………………………………………………** |

**Appendix 1 – The Services to be performed by the Data Processor**