

For use where UH is the controller and the other party is the processor

[Guidance Note: These provisions are to be used when UH is the Controller in relation to Personal Data and is contracting with another party (eg a service provider) as a result of which the other party will process personal data as a Processor on behalf of UH as Controller. Please note that this Agreement does not contain terms allowing transfer outside the EEA, which must be added where such transfer of Personal Data is envisaged.]

Data Access and Sharing Agreement (the “Agreement”)

Parties:

- (1) **UNIVERSITY OF HERTFORDSHIRE HIGHER EDUCATION CORPORATION**, a university in England incorporated pursuant to the Education Reform Act 1988 whose principal office is at College Lane, Hatfield, Hertfordshire, AL10 9AB (the “**University**”);
- (2) [***] registered number [***] whose registered office is at [***] (the “**Service Provider**”), each referred to as a “**Party**” or, together, as the “**Parties**”.

BACKGROUND:

- (A) The University and the Service Provider have entered into a contract for the provision of [***].
- (B) The University would like to share data with the Service Provider and the Parties will act as Data Controller and Data Processor in accordance with the terms and conditions of this Agreement.

1 Definitions and Interpretation

1.1 In this Agreement, the following definitions shall apply:

"Applicable EU Law"	means any law of the European Union (or the law of one or more of the Member States of the European Union);
“Business Hours”	Means 8.30am to 5.00pm on a Working Day;
"Controller", "Processor" and "Data Subject"	shall have the meaning given to those terms in the applicable Data Protection Laws;
"Data Protection Impact Assessment"	means an assessment of the impact of the envisaged Processing operations on the protection of Personal Data, as required by Article 35 of the GDPR;

"Data Protection Laws"	means (a) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a Party is subject, including the Data Protection Act 1998 (" DPA ") and EC Directive 95/46/EC (the " DP Directive ") (up to and including 24 May 2018) and on and from 25 May 2018, the GDPR and all legislation enacted in the UK in respect of the protection of personal data as well as the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (b) any code of practice or guidance published by the ICO (or equivalent regulatory body) from time to time;
"Data Processing Particulars"	means, in relation to any Processing under this Agreement: (a) the subject matter and duration of the Processing; (b) the nature and purpose of the Processing; (c) the type of Personal Data being Processed; and (d) the categories of Data Subjects;
"Data Subject Request"	means an actual or purported request or notice or complaint from or on behalf of a Data Subject exercising his rights under the Data Protection Laws in relation to Personal Data including without limitation: the right of access by the Data Subject, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability and the right to object;
"Effective Date"	has the meaning given in the Schedule;
"Expiry Date"	has the meaning given in the Schedule;
"GDPR"	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1, 4.5.2016;
"Good Industry Practice"	means, at any time, the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would be reasonably expected at such time from a leading and expert [supplier of similar services to those being carried out under this Agreement, such supplier] [amend to fit the agreement] seeking to comply with its contractual obligations in full and complying with all applicable laws (including the Data Protection Laws);
"ICO"	means the UK Information Commissioner's Office, or any successor or replacement body from time to time;
"ICO Correspondence"	means any correspondence or communication (whether written or verbal) from the ICO in relation to the Processing of Personal Data;
"Insolvent"	means a Party: (a) proposes or passes a resolution for its winding up or in the case of a limited liability partnership proposes or determines that it will be wound up; (b) is subject to an application to or order or notice issued by a court or other authority of competent jurisdiction for its winding up or striking off;

- (c) enters administration or is the subject of an application for administration filed at any court or a notice of intention to appoint an administrator given by any person filed at any court;
- (d) proposes, makes or is subject to, a company voluntary arrangement or a composition with its creditors generally, an application to a court of competent jurisdiction for protection from its creditors generally or a scheme of arrangement under Part 26 Companies Act 2006;
- (e) has a receiver or a provisional liquidator appointed over any of its assets, undertaking or income;
- (f) ceases to trade or appears, in the reasonable opinion of the other Party, to be likely to cease to trade;
- (g) is unable to pay its debts within the meaning of section 123 Insolvency Act 1986; or
- (h) is the subject of any event that is equivalent or similar to any events mentioned in sub-clauses (a) to (g) above;

"Losses"	means all losses, fines, penalties, liabilities, damages, costs, charges, claims, amounts paid in settlement and expenses (including legal fees (on a solicitor/client basis), disbursements, costs of investigation (including forensic investigation), litigation, settlement (including ex gratia payments), judgment, interest and penalties), other professional charges and expenses, disbursements, cost of breach notification including notifications to the data subject, cost of complaints handling (including providing data subjects with credit reference checks, setting up contact centres (eg call centres) and making ex gratia payments), all whether arising in contract, tort (including negligence), breach of statutory duty or otherwise;
"Permitted Purpose"	means the purpose of the Processing as specified in the Data Processing Particulars;
"Personal Data"	means any personal data (as defined in the Data Protection Laws) Processed by either Party in connection with this Agreement, and for the purposes of this Agreement includes Sensitive Personal Data (as such Personal Data is more particularly described in Appendix A (<i>Data Processing Particulars</i>));
"Personal Data Breach"	has the meaning set out in the Data Protection Laws and, for the avoidance of doubt, includes a breach of clause 2.2.1(d);
"Personal Data Breach Particulars"	means the information that must be included in a Personal Data Breach notification, as set out in Article 33(3) of the GDPR;
"Personnel"	means all persons engaged or employed from time to time by the Service Provider in connection with this Agreement, including employees, consultants, contractors and permitted agents;

"Processing"	has the meaning set out in the Data Protection Laws (and "Process" and "Processed" shall be construed accordingly);
"Purpose"	has the meaning given in the Schedule;
"Restricted Country"	means a country, territory or jurisdiction outside the European Economic Area which the EU Commission has not deemed to provide adequate protection in accordance with Article 25(6) of the DP Directive and/ or Article 45(1) of the GDPR (as applicable);
"Security Requirements"	means the requirements regarding the security of Personal Data, as set out in the Data Protection Laws (including, in particular, the seventh data protection principle of the DPA and/ or the measures set out in Article 32(1) of the GDPR (taking due account of the matters described in Article 32(2) of the GDPR)) as applicable;
"Sensitive Personal Data"	means Personal Data that reveals such special categories of data as are listed in Article 9(1) of the GDPR;
"Services"	means [Guidance Note: describe the Services to be provided in relation to which the Personal Data will be Processed.] ;
"Services Agreement"	means the agreement relating to the provision of Services dated [] between the University (1) and the Service Provider (2);
"Third Party Request"	means a written request from any third party for disclosure of Personal Data where compliance with such a request is required or purported to be required by law or regulation; and
"Working Day"	means any day except Saturday or Sunday or any bank holiday in England and any other day on which the Parties are officially closed for business.

1.2 In this agreement:

- 1.2.1 unless the context otherwise requires, words in the singular include the plural and vice versa, a reference to a person includes a reference to natural persons, corporate bodies and unincorporated bodies (whether or not having separate legal personality), and a reference to one gender includes a reference to the other genders;
- 1.2.2 clause headings are for ease of reference only and do not form part of the agreement and will not be taken into account when construing it;
- 1.2.3 references to clauses or schedules are to the clauses of or schedules to this agreement;
- 1.2.4 the schedules form part of this agreement and shall have effect as if set out in full in the body of this agreement and any reference to this agreement includes the schedules;
- 1.2.5 a reference to any statute or statutory provision is a reference to that statute or statutory provision as from time to time amended, extended, re-enacted or consolidated (whether before, on or after the date of the agreement), and to all statutory instruments or orders or other subordinate legislation made pursuant to it from time to time; and

- 1.2.6 any words following the terms including, include, in particular or any similar expression will be construed as illustrative and will not limit the sense of the words, description, definition, phrase or term preceding those terms.**

2 Data Protection

2.1 Arrangement between the parties

- 2.1.1 The Parties shall each Process the Personal Data. The Parties acknowledge that the factual arrangements between them dictate the classification of each Party in respect of the Data Protection Laws. Notwithstanding the foregoing, the Parties anticipate that, in respect of the Personal Data, as between the University and the Service Provider for the purposes of this Agreement, the University shall act as the Controller and the Service Provider shall act as the Processor, as follows:
- a The University shall be the Controller where it is Processing Personal Data in relation to **[insert description of purpose]**; and
 - b The Service Provider shall be the Data Processor where it is Processing Personal Data in relation to the Permitted Purpose in connection with the performance of its obligations under this Agreement.
- 2.1.2 Each of the Parties acknowledges and agrees that the Schedule (*Data Processing Particulars*) to this Agreement is an accurate description of the Data Processing Particulars.
- 2.1.3 Nothing within this Agreement relieves the Service Provider of its own direct responsibilities and liabilities under the Data Protection Laws.
- 2.1.4 Each Party shall make due notification to any relevant Regulator.
- 2.1.5 The Service Provider undertakes to the University that it will take all necessary steps to ensure that it operates at all times in accordance with the requirements of the Data Protection Laws and the Service Provider will, at its own expense, assist the University in discharging its obligations under the Data Protection Laws as more particularly detailed in this clause 0 (Data Protection). The Service Provider shall not, whether by act or omission, cause the University to breach any of its obligations under the Data Protection Laws.

2.2 Data Processor Obligations

- 2.2.1 To the extent that the Service Provider Processes any Personal Data as a Processor for and on behalf of the University (as the Controller) it shall:
- a only Process the Personal Data for and on behalf of the University for the purposes of performing its obligations under this Agreement, and only in accordance with the terms of this Agreement and any instructions from the University;
 - b keep a record of any Processing of the Personal Data it carries out on behalf of the University;

- c unless prohibited by law, notify the University immediately (and in any event within twenty-four (24) hours of becoming aware of the same) if it considers, in its opinion (acting reasonably) that it is required by Applicable EU Law to act other than in accordance with the instructions of the University including where it believes that any of the University's instructions under clause 2.2.1(a) infringe any of the Data Protection Laws;
- d take, implement and maintain appropriate technical and organisational security measures which are sufficient to comply with:
 - i at least the obligations imposed on the University by the Security Requirements; and
 - ii the obligations set out in the Schedule relating to security; **[Guidance Note: We should include reference to additional information sharing arrangements/technical security requirements if applicable]**

and where requested provide to the University evidence of its compliance with such requirements promptly, and in any event within forty-eight (48) hours of the request;

- e hold the Personal Data in such a manner that it is capable of being distinguished from other data or information processed by the Service Provider; **[Guidance Note: this is not a strict requirement under the GDPR so we may decide we do not require this]**
- f within thirty (30) calendar days of a request from the University, allow its data processing facilities, procedures and documentation to be submitted for scrutiny, inspection or audit by the University (and/ or its representatives, including its appointed auditors) in order to ascertain compliance with the terms of this clause 2.2 (Data Protection), and provide reasonable information, assistance and co-operation to the University, including access to relevant Personnel and/ or, on the request of the University, provide the University with written evidence of its compliance with the requirements of this clause 2.2 (Data Protection); **[Guidance Note: This provision can be removed if there is an equivalent audit provision elsewhere in the Agreement and it is wide enough to cover the audit of the Service Provider with respect to its compliance with these data protection obligations.]**
- g not disclose Personal Data to a third party (including a sub-contractor) in any circumstances without the University's prior written consent, save in relation to Third Party Requests where the Service Provider is prohibited by law or regulation from notifying the University, in which case it shall use reasonable endeavours to advise the University in advance of such disclosure and in any event as soon as practicable thereafter;
- h promptly comply with any request from the University to amend, transfer or delete any Personal Data;

- i notify the University promptly (and in any event within forty-eight (48) hours) following its receipt of any Data Subject Request or ICO Correspondence and shall:
 - i not disclose any Personal Data in response to any Data Subject Request or ICO Correspondence without first consulting with and obtaining the University's prior written consent; and
 - ii provide the University with all reasonable co-operation and assistance required by the University in relation to any such Data Subject Request or ICO Correspondence;

- j notify the University immediately upon becoming aware of any actual or suspected, threatened or 'near miss' Personal Data Breach in relation to the Personal Data (and follow-up in writing) and shall: **[Guidance Note: The wording 'near miss' is intended to capture the symptoms of a system vulnerability that could lead to a personal data breach if not remedied. However, it may cause concern for the Data Processor as it may lead to notification of a high volume of low risk incidents. Therefore, this wording may be deleted if the Data Processor objects (with justification) to its inclusion.]**
 - i conduct or support the University in conducting such investigations and analysis that the University reasonably requires in respect of such Personal Data Breach;
 - ii implement any actions or remedial measures necessary to restore the security of compromised Personal Data; and
 - iii assist the University to make any notifications to the ICO and affected Data Subjects;

- k comply with the obligations imposed upon a Processor under the Data Protection Laws;

- l use all reasonable endeavours, in accordance with Good Industry Practice, to assist the University to comply with the obligations imposed on the University by the Data Protection Laws, including:
 - i compliance with the Security Requirements;
 - ii obligations relating to notifications required by the Data Protection Laws to the ICO and/ or any relevant Data Subjects;
 - iii undertaking any Data Protection Impact Assessments (and, where required by the Data Protection Laws, consulting with the ICO and/or any other relevant Regulator in respect of any such Data Protection Impact Assessments); and
 - iv without undue delay and where feasible not later than 72 hours after having become aware of it notify Personal Data Breaches to the ICO and/or any other relevant Regulator unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons;

- m Upon the earlier of:
 - i termination or expiry of this Agreement (as applicable); and
 - ii the date on which Personal Data is no longer relevant to, or necessary for, the Permitted Purpose

the Service Provider shall cease Processing all Personal Data and return and/or permanently and securely destroy so that it is no longer retrievable (as directed in writing by the University) all Personal Data and all copies in its possession or control and, where requested by the University, certify that such destruction has taken place (promptly, and in any event within forty-eight (48) hours of the request) except to the extent required by Applicable EU Law to retain the Personal Data;

- n not make (nor instruct or permit a third party to make) a transfer of any Personal Data to a Restricted Country except with the prior written consent of the University and in accordance with any terms the University may impose on such transfer as the University deems necessary to satisfy the requirements to ensure that transfers of Personal Data outside of the EEA have adequate protections in place as set out in the Data Protection Laws. **[Guidance: where there is transfer of Personal Data outside the EEA, additional terms will need to be added to this Agreement to ensure that such transfer meets GDPR requirements. Appropriate terms are set out in Appendix VI to the Data Protection UPR.]**

2.2.2 Except as otherwise provided, this Agreement does not transfer ownership of, or create any licences (implied or otherwise), in any intellectual property rights in any Personal Data.

2.3 Supplier Personnel

2.3.1 The Service Provider shall only disclose Personal Data to its Personnel that are required by the Service Provider to assist it in meeting its obligations under this Agreement (the "**Project Personnel**") and shall ensure that no other Personnel shall have access to such Personal Data.

2.3.2 The Service Provider shall only disclose Personal Data to the Project Personnel where the following conditions have been satisfied in relation to such Project Personnel:

- a the Service Provider shall have taken (and shall continue to take) all reasonable steps to ensure the reliability and integrity of each member of the Project Personnel;
- b each member of the Project Personnel shall have been subject to adequately clear pre-employment checks;
- c each member of the Project Personnel shall have undergone, and shall continue to receive on an annual basis, reasonable levels of training in Data Protection Laws and in the care and handling of Personal Data; and
- d each member of the Project Personnel shall have entered into appropriate contractually-binding confidentiality undertakings.

2.4 Appointing Sub-contractors

2.4.1 The Service Provider shall not sub-contract the performance of any of its obligations under this Agreement without the prior written consent of the University. Where The Service Provider has such consent, it shall be permitted to appoint a sub-contractor in accordance with this clause 2.4 and to disclose Personal Data to such sub-contractor for Processing in accordance with the Service Provider's obligations under this Agreement, provided always that:

- a the Service Provider undertakes thorough due diligence on the proposed sub-contractor, including a risk assessment of the information governance-related practices and processes of the proposed sub-contractor, which shall be used by the Service Provider to inform any decision on appointing the proposed sub-contractor;
- b the Service Provider provides the University with full details of the proposed sub-contractor including the results of the due diligence undertaken in accordance with clause 2.4.1(a) before its appointment and the University has consented to such appointment in writing;
- c the sub-contractor contract (as it relates to the Processing of Personal Data) is on terms which are substantially the same as, and in any case no less onerous than, the terms set out in this Agreement;
- d the sub-contractor's right to Process Personal Data terminates automatically on expiry or termination of this Agreement for whatever reason. **[Guidance Note: This provision is not appropriate for cloud/ one to many service provisions.]**

2.4.2 Notwithstanding any consent or approval given by the University under clause 2.4.1, the Service Provider shall remain primarily liable to the University for the acts, errors and omissions of any sub-contractor to whom it discloses Personal Data, and shall be responsible to the University for the acts, errors and omissions of such sub-contractor as if they were the Service Provider's own acts, errors and omissions to the extent that the Service Provider would be liable to the University under this Agreement for those acts, errors and omissions.

2.4.3 This Agreement shall continue in full force and effect for so long as the Service Provider Processes any Personal Data.

3 Indemnity

3.1 The Service Provider shall indemnify on demand and keep indemnified the University from and against:

- 3.1.1 any monetary penalties or fines levied by the ICO and/or any other Regulator on the University;
- 3.1.2 the costs of an investigative, corrective or compensatory action required by the ICO and/or any other Regulator, or of defending proposed or actual enforcement taken by the ICO and/or any other Regulator;

- 3.1.3 any Losses suffered or incurred by, awarded against, or agreed to be paid by, the University pursuant to a claim, action or challenge made by a third party against the University (including by a Data Subject); and
- 3.1.4 except to the extent that clauses 0 and/or 0 and/or 0 apply, any Losses suffered or incurred, awarded against, or agreed to be paid by, the University; in each case to the extent arising as a result of a breach by the Service Provider (or its sub-contractors) of this Agreement and/or their respective obligations under the Data Protection Laws.
- 3.2 Nothing in this Agreement will exclude, limit or restrict the Service Provider's liability under the indemnity set out in clause 0.

4 Insurance

- 4.1 The Service Provider agrees:
 - 4.1.1 to obtain and keep in full force and effect at all times a policy or policies of insurance which meets the following conditions:
 - a it must cover liability for damage arising to any person;
 - b it must apply in relation to the Processing of Personal Data; and
 - c it must have policy limits and provisions conforming to such requirements as the University may from time to time reasonably prescribe;
 - 4.1.2 to deliver to the University:
 - a copies of all applicable insurance policies taken out pursuant to the provisions of this Agreement; and
 - b evidence of premiums paid in relation to such insurance; and
 - 4.1.3 to ensure that the University shall be entitled to the benefit under such insurance and (where the University so requires) that the University's interest will be noted on the policy.

5 Access to University to Servers

- 5.1 In the event that the Service Provider requires access to the University's IT servers and/or other IT infrastructure to enable it to perform the relevant provisions of the Services Agreement it shall notify the University of its requirements in writing. If the University grants the Service Provider access to its IT servers and/or other IT infrastructure, the Service Provider confirms that it, together with any sub-contractor instructed by it, will only access the IT servers and/or other IT infrastructure in accordance with the terms of this Agreement and the University's IT Server Access Guidelines which will be made available to the Service Provider upon request. Failure by the Service Provider to comply with the terms of this clause 5.1 (Access to University IT Servers) will constitute a material breach under clause 6.5 (Termination). **[Guidance: We should consider carefully whether this provision is or is likely to be required. Access to University IT servers should only be granted where absolutely necessary.]**

6 Termination

- 6.1 Subject to earlier termination in accordance with this clause 6 (Termination), this Agreement shall come into force on the Effective Date and shall remain in force until the Expiry Date.
- 6.2 If the Service Provider wishes to retain the Personal Data beyond the Expiry Date, it must contact the University not less than one month prior to the Expiry Date to seek an extension of this Agreement. Under no circumstances shall the Service Provider retain the Personal Data without an appropriate data sharing agreement relating to the Personal Data being in place.
- 6.3 The University may terminate this Agreement for any reason by giving the Service Provider not less than one (1) month's prior written notice.
- 6.4 On or at any time after the occurrence of a Personal Data Breach, the University shall be entitled to terminate this Agreement with immediate effect by written notice to the Service Provider.
- 6.5 The University may terminate this Agreement immediately if:
- 6.5.1 the Service Provider is in material breach of this Agreement and that breach cannot be remedied;
 - 6.5.2 the Service Provider is in material breach of this Agreement and that breach can be remedied but the Service Provider has failed to do so within twenty (20) Working Days starting on the day after receipt of written notice from the University;
 - 6.5.3 in respect of Personal Data, the Service Provider no longer has a legal basis on which to Process the Personal Data;
 - 6.5.4 the Service Provider becomes Insolvent;
 - 6.5.5 it becomes unlawful for the Service Provider to perform all or any of its obligations under the Services Agreement and/or this Agreement; or
 - 6.5.6 there is a change in the Data Protection Laws which materially affects the University's powers to provide Personal Data to the Service Provider.
- 6.6 Without prejudice to any other right available to the University, where the Service Provider (or any sub-contractor engaged by the Service Provider) either (a) commits or causes a breach of this Agreement, or (b) is responsible for a Personal Data Breach, the University may suspend this Agreement without incurring any liability to the Service Provider, with immediate effect by written notice to the Service Provider.

7 Effect of Termination

- 7.1 The service of notice to terminate under clause 5 (Termination) will not absolve the Service Provider of its obligations to comply fully with the terms and conditions of this Agreement until such termination is effective and will be without prejudice to the rights the University may have accrued up to the date of termination.

- 7.2 Upon termination or expiry of this Agreement for any reason, the Service Provider shall:
- 7.2.1 immediately cease all use of and, at the University's option, either return or destroy all the Personal Data and any other data disclosed to it by the University, and shall procure the compliance with this obligation of any permitted sub-contractor; and
- 7.2.2 provide the University, within five (5) Working Days from the date of termination or Expiry Date, with a certificate given by an officer of the Service Provider declaring that all the Personal Data and any other data disclosed to it by the University in the Service Provider's possession or control has been returned or destroyed as applicable and that no Personal Data or such other data (or any copies thereof) has been retained by the Service Provider.
- 7.3 Unless otherwise provided for and subject to any rights and obligations which may have accrued prior to termination or expiry, neither Party will have any further obligation to the other under this Agreement.
- 7.4 The following clauses will survive termination or expiry of this Agreement: clauses 1 (Definitions and Interpretation), 2 (Data Protection), 3 (Indemnity), 7 (Effect of Termination), 9 (Dispute Resolution), and 10 (General Provisions) and any other provisions that are expressly stated or impliedly understood to survive termination or expiry of this Agreement.

8 Notices

- 8.1 A notice given under this Agreement will be:
- 8.1.1 sent for the attention of the person, and to the address, given in this clause 8 (Notices) (or such other address or person as the relevant party may notify to the other parties); and
- 8.1.2 delivered personally; or
- 8.1.3 delivered by commercial courier; or
- 8.1.4 sent by pre-paid United Kingdom first-class post or recorded delivery.
- 8.2 The addresses for service of notice are:
- 8.2.1 The University of Hertfordshire, College Lane, Hatfield, Hertfordshire, AL10 9AB. For the attention of: The Secretary and Registrar.
- 8.2.2 The Service Provider, **[address]**. For the attention of: **[named officer]**.
- 8.3 If a notice has been properly sent or delivered in accordance with this clause 8 (Notices), it will be deemed to have been received as follows:
- 8.3.1 if delivered personally, at the time of delivery; or
- 8.3.2 if delivered by commercial courier, at the time of signature of the courier's delivery receipt; or

- 8.3.3 if sent by pre-paid United Kingdom first class post to an address in the United Kingdom, 48 hours after it was posted; or
- 8.3.4 if deemed receipt under any of sub-clauses 8.3.1 to 8.3.4 (inclusive) is not within Business Hours, receipt will be deemed on the Party's next Working Day.
- 8.4 In proving service in respect of personal delivery or delivery by post it will be sufficient to prove that the envelope containing such notice was addressed to the correct address of the relevant party and delivered to that address.

9 Dispute Resolution

- 9.1 If a dispute arises out of or in connection with this Agreement or the performance, validity or enforceability of it (a “**Dispute**”), then, except as expressly provided in this Agreement, the Parties shall follow the procedure set out in this clause:
 - 9.1.1 either Party shall give to the other written notice of the Dispute, setting out its nature and full particulars (a “**Dispute Notice**”), together with relevant supporting documents. On service of the Dispute Notice, the Secretary and Registrar of the University (or their nominee) and [**insert employee title of the individual who will initially deal with disputes**] of the Service Provider (hereinafter referred to as the “**First Stage Representatives**”) shall attempt in good faith to resolve the Dispute (the “**First Stage Negotiation**”);
 - 9.1.2 if the First Stage Representatives are for any reason unable to resolve the Dispute within forty (40) Working Days of it being referred to them, the Parties agree to enter into mediation in good faith to settle the Dispute in accordance with the CEDR Model Mediation Procedure, or in the event that CEDR has ceased to exist, in accordance with the model procedure of an independent service provider specialising in the resolution of conflict deadlock. Unless otherwise agreed between the Parties within ten (10) Working Days of the completion of the First Stage Negotiation, the mediator shall be nominated by CEDR. To initiate the mediation, a Party must serve notice in writing (the “**ADR Notice**”) to the other Party to the Dispute, referring the dispute to mediation. Unless otherwise agreed between the Parties, and subject to any constraints imposed by CEDR, the mediation will start not later than fifteen (15) Working Days after the date of the ADR Notice.
- 9.2 No Party may commence any court proceedings under clause 9.3 in relation to the whole or part of the Dispute until twenty (20) Working Days after service of the ADR Notice, provided that the right to issue proceedings is not prejudiced by a delay. Nothing in this clause 9.2 will prevent either Party from seeking injunctive or similar relief at any time.
- 9.3 If the Dispute is not resolved within forty (40) Working Days after service of the ADR notice, or either Party fails to participate or ceases to participate in the mediation before the expiry of that 40-Working Day period, or the mediation terminates before the expiry of that 40-Working Day period, the Dispute may be finally resolved by the courts of England and Wales in accordance with clause 10.9 of this Agreement.

10 General Provisions

- 10.1 The Service Provider does not have the right to assign, transfer, sub-contract, charge, or deal in any other manner with any of its rights and/or obligations under this Agreement, or any right arising under it, without the prior written consent of the University.
- 10.2 This Agreement contains the entire agreement between the Parties with respect to the subject matter hereof, and supersedes all previous discussions, agreements, arrangements and understandings between the Parties with respect thereof. Each Party acknowledges that in entering this Agreement it has not relied on, and will have no right or remedy in respect of, any statement, representation, assurance or warranty (whether made negligently or innocently) other than as expressly set out in this Agreement. Nothing in this clause 10.2 will limit or exclude any liability for fraud.
- 10.3 No variation of this Agreement will be effective unless it is in writing and signed by authorised representatives of both Parties.
- 10.4 If any provision of this Agreement will be held to be unlawful, invalid or unenforceable, in whole or in part, under any enactment or rule of law, such provision or part will to that extent be severed from this Agreement and rendered ineffective as far as possible without modifying or affecting the legality, validity or enforceability of the remaining provisions of this Agreement which will remain in full force and effect.
- 10.5 No person who is not a Party to this Agreement will have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement but this does not affect any right or remedy of a third party which exists or is available apart from that Act.
- 10.6 The failure of either Party at any time to enforce any of the provisions of this Agreement or exercise any right under this Agreement will not operate as a waiver of that right or preclude the exercise or enforcement of it at any time or times thereafter.
- 10.7 This Agreement may be entered into by the Parties in separate counterparts, each of which so executed and delivered will be an original, but all the counterparts will together constitute one and the same instrument.
- 10.8 This Agreement, and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims), shall be governed by, and construed in accordance with, the law of England and Wales.
- 10.9 The Parties both irrevocably agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims).

Appendix A - Data Processing Particulars

INFORMATION REQUIRED UNDER THE DATA PROTECTION LAWS	
The subject matter and duration of the Processing	
The nature and Purpose of the Processing	
The categories of Data Subjects	

[Guidance Note: The above information is required by the GDPR (Article 28(3)) which requires data processing agreements to include details of the subject-matter, duration, nature and purpose of the processing and the type of personal data and categories of data subjects involved in the data processing.]

A. GENERAL PARTICULARS		
1.1 Name(s) and job title(s) of the nominated person(s) at the Service Provider for receiving the Personal Data from the University (Please note that all data access must be by named individual only)		
1.2 Nature of Service Provider’s relationship/arrangement/partnership with the University		
1.3 The purpose(s) for which the data access or sharing is required (the “ Purpose ”): Enabling the Service Provider to perform (as Service Provider) certain functions which are obligations of the Service Provider under the Services Agreement.		
1.4 Agreement Effective Date (“ Effective Date ”):		
1.5 Agreement Expiry Date (“ Expiry Date ”): (subject to earlier termination under clause Error! Reference source not found. (Termination))		
1.6 Type(s) of	Personal Data	<i>[list all types of personal data shared]</i>

data	Sensitive (special category) Personal Data	<i>[list all types of sensitive personal data shared, as defined by the Data Protection Laws]</i>
	statistical / other data	<i>[describe other data shared, including company confidential and anonymised data]</i>
1.7 Method(s) of transfer	shared access	<i>[describe any arrangements for access to University systems to facilitate data sharing]</i>
	physical transfer	<i>[describe any arrangements for sending and receiving data to/from the University, including encryption (compulsory)]</i>
	electronic transfer	<i>[describe any arrangements for electronic transfer of data to/from the University, including encryption (compulsory)]</i>
B. SECURITY		
1.8 Security provisions	designated responsibilities	<i>[describe responsibilities for providing the data and who will have access to it]</i>
	encryption	<i>[describe whether the data will be encrypted in transit or at rest and if so the encryption methods that will be used]</i>
	formats used	<i>[list types of removable media and data file/attachment formats used]</i>
	access	<i>[describe the security arrangements for the Service Provider's access to University data sources]</i>
1.9 Storage provisions	<i>[where data is being transferred to the Service Provider, describe the data storage arrangements to be provided by the Service Provider, including hosting arrangements and cyber security provisions in place]</i>	
1.10 Records created	<i>[describe any records created by the data sharing relationship, including any requirements for creating and storing meeting papers, reports and joint publications]</i>	
1.11 Data / record deletion	<i>[describe the arrangements for data / record deletion and/or archiving during and on termination of the Agreement]</i>	

FOR OFFICE USE ONLY
(block capitals)

Job Title:

Signed:

Name:

Signed:

Agreement No:Name:

Data Steward for:

Date:

Chief Information Officer

Date:

For **UNIVERSITY OF HERTFORDSHIRE HIGHER EDUCATION CORPORATION:**

Name: MRS SHARON HARRISON-BARKER

(block capitals)

Position: Secretary and Registrar

Signed:

Date:

For **[Insert full legal name of Service Provider]**

Name:

(block capitals)

Position:

Signed:

Date:

Sharon Harrison-Barker

Secretary and Registrar

Signed: **15 October 2021**

Alternative format

If you need this document in an alternative format, please email us at governanceservices@herts.ac.uk or telephone us on +44 (0)1707 28 6006.