DATA PROCESSING AGREEMENT

THIS AGREEMENT is made the _____day of_____(Year)
BETWEEN

THE UNIVERSITY OF DURHAM whose legal address is The Palatine Centre, Stockton Road, Durham, DH1 3LE ("the University"); and

[INSERT] whose legal address [INSERT] ("Data Processor");

WHEREAS:

A. The Data Processor has been selected by the University to process certain data for the purposes of [INSERT] (the "Activity").

B. The Parties acknowledge that in order for the Data Processor to undertake the Activity, it will be necessary for the University to share certain personal data relating to third parties with the Data Processor.

C. The Parties wish to define their rights and responsibilities in respect of the sharing and processing of that information, with particular regard to the Parties' obligations under applicable Data Protection Legislation.

IT IS HEREBY AGREED AS FOLLOWS:-

1. Interpretation

1.1 In this Agreement the following terms shall have the following meanings:

"Data Controller"	means the University of Durham;
"Data Processor"	means the Party identified at the head of this Agreement who shall be Processing personal Data on behalf of the Data Controller.
"Data Protection Legislation"	means the Data Protection Act 2018, the Regulation EU/2016/679 of the European Parliament and of the Council of 27 April 2016 (the General Data Protection Regulation) and all applicable laws and regulations relating to processing of personal data and privacy including where applicable the mandatory guidance and mandatory codes of practice issued by the Information Commissioner;
"Data Subject"	means as defined in Data Protection Legislation;

"Permitted Purpose"	the purpose for which the Data Processor shall be permitted by the Data Controller to process University Data in connection with the Activity, namely [insert]/
"Recipients"	permitted third party recipients of University Data;
"University End User**"**	means an individual employed by the University and assigned to the Activity who shall be entitled to access any University Data on behalf of the University;
"The Personal Data"	means the following categories of Personal Data belonging to Data Subjects, which will be shared with the Data Processor for the Purposes set out herein: **[Please enter personal data to be processed, for example** **Name** **Address** **Age** **Gender** **Identification number]** The following Special Categories of Personal Data may be included (as appropriate): ***[Please delete where not applicable]*** ***Racial or ethnic origin*** ***Political opinions*** ***Religious or philosophical beliefs*** ***Trade Union Membership*** ***Health*** ***Sex life or sexual orientation*** ***Genetic data*** ***Biometric data.***

2. GENERAL

2.1 This Agreement shall be deemed to commence on the date of signature of this Agreement and shall continue in full force and effect until **[INSERT]** unless earlier terminated in accordance with the terms set out herein.

2.2 It is acknowledged by the Parties that the Activity may include a requirement of the Data Processor to process The Personal Data which may contain a substantial amount of Special Categories of Personal Data (as defined in Data Protection legislation), and as a consequence, the Data Processor shall pay particular attention to the provisions of the following Clauses.

2.3 As defined in Data Protection Legislation, for the purposes of the Activity, the University shall be considered the Data Controller of all The Personal Data and the Data Processor shall be Data Processor acting on the University's behalf. The University is

a higher education institution engaging in the provision of higher education services and facilities. The Data Processor will only act upon the University's documented instructions, including with regard to transfers of The Personal Data to a third country or international organisation, unless required to do so by Union or Member State law, in which case the Data Processor shall inform the University of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

2.4 The Data Processor shall immediately inform the University if, in its opinion, an instruction infringes the GDPR or other Data Protection Legislation.

2.5 The Data Processor shall, at its election and as necessary assist the Data Controller to ensure its compliance with its obligations under Article 28 of the General Data Protection Regulation.

2.6 The Data Processor shall at all times ensure it complies with all Data Protection Legislation applicable to the Data Processor's provision of the Activity to the University and the University handling of any relevant Personal Data.

3 PROCESSING, USE AND ACCESS TO THE PERSONAL DATA

3.1 The Data Processor warrants to the University that for the duration of this Agreement the Data Processor shall, and shall procure that its directors, employees, agents, and representatives shall, process The Personal Data only as outlined in the specification and in strict compliance with the terms of this Agreement.

3.2 The Data Processor shall ensure its personnel will not process The Personal Data without authorisation, and only those of the Data Processor's personnel who are bound under obligations to maintain the confidentiality of The Personal Data no less stringent than those contained herein, and such obligations shall continue even following termination of their engagement with the Data Processor.

3.3 In supplying the Activity hereunder, the Data Processor acknowledges and agrees the following:

3.3.1 The Data Processor shall at no point use or disclose any of The Personal Data transferred hereunder for any purpose other than the Permitted Purpose expressly defined herein.

3.3.2 The Data Processor is hereby authorised to use The Personal Data only for the Permitted Purpose in connection with the Activity. Where strictly required for the continued provision of the Activity, The Personal Data may be used by the Data Processor only to the extent necessary to prevent, detect and repair problems affecting the operation of the Activity and where required for the detection of, and protection against, emerging and evolving threats to the security and/or integrity of The Personal Data.

3.3.3 The Data Processor shall inform the Data Controller whether other Data processors are involved in the provision of the services. The list of other processors ('the Approved Sub-processors') is attached hereto as Schedule 1.

3.4 The Data Processor shall not engage another Processor without the written authorisation of the Data Controller. Where this is authorised,

3.4.1 a legally binding contract is put in place with the sub-processor which contains obligations in relation to the processing of The Personal Data as required by Article 28 of the GDPR and, in particular, providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR and

3.4.2 where the sub-processor fails to fulfil its data protection obligations, the Data Processor shall remain fully liable to the University for the performance of that sub-processor's obligations.

3.5 The Data Processor shall, taking into account the nature of the processing, assist the University by appropriate technical and organisational measures, insofar as this is possible (and subject to the applicable fees and service levels stated in any agreement for services), for the fulfilment of the University's obligation to respond to requests for exercising the rights of Data Subjects laid down in Chapter III of the GDPR. In this regard, in the event that any Data Subject should contact the Data Processor directly with a request to exercise their individual rights under Data Protection legislation, the Data Processor shall request that such Data Subject redirect such request and submit such request directly to the University using the info.access@durham.ac.uk email address. For the purposes of this Clause 3.5, the Data Processor may provide to said Data Subject the University's basic contact information to which such request should be made.

3.6 The Data Processor shall assist the University in ensuring compliance with the obligations pursuant to Articles 32 to 36 (inclusive) of the GDPR taking into account the nature of the processing and the information available to the Data Processor.

3.7 The Data Processor shall make available to the University all information reasonably necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR in respect of The Personal Data and allow for and contribute to audits, including inspections, conducted by or on behalf of the University (at the cost of the University).

3.8 The Data Processor shall not unilaterally grant any University End User access to any of The Personal Data outside those considered expressly to be part of the Activity provided hereunder as confirmed by the University from time to time. Neither shall the Data Processor respond to any request for such access made by a University End User outside those considered expressly to be part of the Activity provided hereunder, with the exception of:

3.8.1 where such University End User is determined to be a legally Authorised representative of the University, and such request is made in writing; or

3.8.2 where the Data Processor is compelled to do so under the provisions of an applicable law.

3.9 The Data Processor hereby warrants to the University that it will within one (1) working day, notify the University in the event:

3.9.1 the Data Processor receives any legally binding request for disclosure of The Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

3.9.2 there is any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to The Personal Data; and

3.9.3 any request is received by the Data Processor directly from a subject of The Personal Data. The Data Processor shall not respond to such request directly, unless it has been otherwise authorised by the University to do so.

3.10 For the avoidance of doubt, the Data Processor hereby acknowledges that all The Personal Data supplied to the Data Processor in the course of this Agreement shall at all times remain the sole and exclusive property of the University. Nothing in this Agreement shall be considered to grant to the Data Processor any right or licence to use, access or process The Personal Data, except to the extent that it is necessary for the Data Processor to perform the Permitted Purpose in connection with the Activity in accordance with the terms of this Agreement.

3.11 At the University's choice, the Processor will safely delete or return The Personal Data at any time. Where the Processor is to delete The Personal Data, deletion shall include destruction of all existing copies unless there is a legal requirement to retain The Personal Data. Where there is a legal requirement the Processor will, prior to entering into this Agreement, confirm such an obligation in writing to the University. Upon request by the University the Processor shall provide certification of destruction of all of The Personal Data.

4. CONTROLLER CONFIRMATIONS

4.1 As Data Controller of The Personal Data provided to the Data Processor by the University, the University:

4.1.1 warrants that it is registered as a Data Controller with the Information Commissioner's Office (the ICO) insofar as this is a requirement under the Data Protection Legislation;

4.1.2 shall be responsible for complying with the obligations to which Data Controllers are subject under Data Protection Legislation in respect of The Personal Data, including without limitation:

4.1.2.1 providing to Data Subjects the information referred to in Articles 13 and 14 of the General Data Protection Regulation; and

4.1.2.2 dealing with the exercise by Data Subjects of their rights under the General Data Protection Regulation;

4.1.3 warrants that it has all necessary and appropriate authority and consents to disclose The Personal Data to the Data Processor;

4.1.4 shall promptly notify the Data Processor of any complaint, notice or communication which relates directly or indirectly to the processing of The Personal Data or to either Party's compliance with the Data Protection Legislation and shall not respond to any such complaint, notice or communication without first consulting with the Data Processor.

5. NO EXPORT OF THE PERSONAL DATA

5.1 The Data Processor hereby confirms that the primary and backup facilities for

processing of The Personal Data shall be located in the European Economic Area (EEA). Under no circumstance may the Data Processor export any of The Personal Data outside the EEA in the absence of express written permission of the University. Where the University chooses to grant any such permission, the Data Processor acknowledges additional terms shall be applied to such transfer.

6. INFORMATION SECURITY

6.1 The Data Processor warrants that it has implemented and will continue to maintain for the duration of the Activity appropriate technical and organisational measures, policies, procedures, internal controls, and information security routines intended to protect The Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access as follows:

6.1.1 The Data Processor shall appoint one or more named individuals responsible for coordinating and monitoring the security rules and procedures surrounding handling of The Personal Data;

6.1.2 All Data Processor personnel with access to The Personal Data shall be made subject to confidentiality obligations no less stringent than those contained herein and shall not access or have access to The Personal Data unless appropriately trained in Data Protection and confidentiality to ensure that The Personal Data is handled securely;

6.1.3 The Data Processor shall maintain an asset register for The Personal Data that it processes, including an inventory of all equipment on which The Personal Data is processed;

6.1.4 The Data Processor shall ensure that at all times all The Personal Data is kept appropriately separated and clearly identifiable from any of the Data Processor's data and any data of third parties to whom the Data Processor also provides services;

6.1.5 The Data Processor shall classify The Personal Data in accordance with the University's reasonable instructions to help identify it and to allow for access to it to be appropriately restricted (for example through suitable encryption);

6.1.6 The Data Processor shall impose appropriate restrictions on printing The Personal Data provided to it in electronic or digital format and has adequate procedures in place for secure disposal of printed materials that may contain The Personal Data;

6.1.7 The Data Processor shall ensure that none of its personnel store The Personal Data on any portable device, (for example USB stick or removable media) or process The Personal Data outside the Data Processor's facilities;

6.1.8 The Data Processor shall enforce strong authentication controls to validate the identity and legitimate access to The Personal Data from outside of the Data Processor's designated facilities by any authorised subcontractor or the Data Processor's personnel.

6.1.9 The Data Processor shall implement and shall ensure that any Subcontractors engaged by the Data Processor shall implement appropriate logical and physical security controls so that only authorised personnel are able to access

facilities where information systems that process The Personal Data are located;

6.1.10 The Data Processor shall employ stringent industry standard processes for the secure destruction of The Personal Data beyond recovery. All The Personal Data and related documentation shall be held and disposed of strictly in accordance with the University's instructions (which may be to return The Personal Data and/or documentation to the University).

6.1.11 On commencement of this Agreement, the Data Processor shall maintain and provide the University with all relevant security policies and procedures describing its security measures and designated responsibilities of its personnel who have access to The Personal Data. In the event of any change to the Data Processor's security measures and the relevant procedures and responsibilities of its personnel over the duration of this Agreement, the Data Processor shall promptly notify the University of any such changes and shall provide the University with updated security documents, reflecting any such changes;

6.1.12 The Data Processor shall have a documented security patching policy or procedure and operate to it. The policy or procedure shall include specific reference to patching critical security vulnerabilities in a timely manner based on risk and exposure;

6.1.13 The Data Processor shall store backups of all The Personal Data and data recovery procedures at a different site to where The Personal Data is held (and the primary computer equipment processing The Personal Data is located);

6.1.14 The Data Processor shall review and update data recovery procedures at least once every twelve (12) months for the duration of the Activity;

6.1.15 The Data Processor shall encrypt any The Personal Data that is transmitted over public networks with widely recognised secure protocols and ciphers recognised to be fully up to date and industry standard at the time of any such use;

The Data Processor shall restrict access to any The Personal Data held in any media leaving its storage facilities through appropriate security measures (for example encryption with widely recognised secure protocols and ciphers and long key lengths expected to remain secure for a 10-50 year lifetime or barcode tracker system for paper files);

6.1.16 The Data Processor shall maintain a record of all security privileges of individuals having access to The Personal Data and maintain and update a record of personnel authorised to access Data Processor systems that contain The Personal Data. The Data Processor shall adopt a principle of least privilege and not grant access to The Personal Data to any Data Processor personnel that do not have an explicit business requirement for access. Any staff or accounts that no longer require access will be promptly prevented from accessing The Personal Data;

6.1.17 The Data Processor shall instruct all Data Processor personnel to disable any sessions capable of accessing The Personal Data when leaving premises or when computers are otherwise left unattended;

6.1.18 The Data Processor shall maintain anti-malware controls to prevent malicious software impacting the confidentiality, integrity or availability of The Personal Data, including malicious software originating from public networks;

6.1.19 The Data Processor shall ensure that all access to The Personal Data by Supplier personnel and others is protected by industry standard authentication mechanisms, recognised to be secure at the time of such use;

6.1.20 The Data Processor shall maintain procedures to deactivate accounts and passwords that have been compromised or inadvertently disclosed;

6.1.21 The Data Processor shall use industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage;

6.1.22 The Data Processor shall implement all necessary controls to avoid individuals assuming access rights they have not been assigned, which would provide unauthorised access to The Personal Data. In the event that the Data Processor becomes aware of any such access gained, it shall notify the University within one (1) working day. The Data Processor shall maintain a full record of all information security incidents or weaknesses leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to The Personal Data and shall make such records available to the University for inspection at any time during business hours. Such record shall include a description of the incident or weakness, the time period, the consequences, the name of the reporter and to whom the breach was reported, and the immediate steps taken and longer term actions planned to address the security issues and prevent repetition.

6.1.23 The Data Processor shall maintain emergency and contingency plans in the event of an information security incident or weakness at the facilities or premises of the Data Processor where The Personal Data is located. The Data Processor shall ensure its redundant storage and its procedures for recovering data are designed to attempt to reconstruct The Personal Data in line with agreed Recovery Point Objectives.

7 INFORMATION SECURITY, POLICY, AUDIT AND UPDATES

7.1 The Data Processor has established and agrees to maintain a Data and Information Security Policy and Information Security Management System and appropriate controls. For the establishment, implementation, control, and improvement of the Information Security Management System (the "Data Processor Information Security Policy").

7.2 The Data Processor will audit the security of the environment (including computers and computing environment) that the Data Processor and any of the Data Processor's Subcontracts use in processing The Personal Data (including personal data) in the course of the Activity. Such audit shall be:

7.2.1 performed at least as frequently as once annually for the duration of the Activity;

7.2.2 performed by third party security professionals at the Data Processor's selection and expense; and

7.2.3 used to produce an audit report (the "Data Processor Audit Report"), which will be the Data Processor's confidential information, but shall be provided to the University on written request to allow the University to verify the Data Processor's compliance with the security obligations under this Agreement.

7.3 The Data Processor will operate one or more firewalls (or equivalent network device) installed on the boundary of the Data Processor's internal network(s) restricting inbound and outbound network traffic to authorised connections. Changes allowing network traffic to pass through the firewall must be subject to an approval process. Unapproved services, or services that are typically vulnerable to attack must be blocked by default and unused rules removed.

7.4 Data Processor IT and networked devices must be securely configured with unnecessary user accounts removed or disabled, default passwords changed to strong passwords and unnecessary software and services removed or disabled. Auto-run features should be disabled for removable storage media and host firewalls (or equivalent) should be enabled on end devices blocking inbound connections by default.

7.5 The Data Processor must implement robust malware protection on exposed computers. Malware protection software must be kept up-to-date and configured to scan files automatically upon access and to scan web pages on access and blacklist known malicious sites. Scans of all files should be undertaken regularly.

7.6 Software should be kept up-to-date, as a minimum software should be licensed and supported (by the software vendor or Data Processor of the software) to ensure security patches for known vulnerabilities are made available. Security updates to software must be installed in a timely manner. Out-of-date software (i.e. software that is no longer supported) must be removed.

IN WITNESS WHEREOF, each Party accepts and agrees to the above provisions as of the effective date of this Agreement, and has caused this Agreement to be executed in duplicate by a duly authorised representative.

For and on behalf of the **UNIVERSITY OF DURHAM** by:

Signed: _____

Name: _____

Position: _____

Date: _____

For and on behalf of **DATA PROCESSOR:**

Signed: _____

Name: _____

Position: _____

Date: _____

SCHEDULE 1

LIST OF APPROVED SUB-PROCESSORS

ENTITY (NAME & ADDRESS)	TYPE OF SERVICE PROVIDED	COUNTRY LOCATION