Data Processing Addendum (DPA)

Part A: Personal Data to be Shared and/or Transferred

		Details
Types of personal data	**Personal Data**	As specified in the Contract, but may include (without limitation) name, address, date of birth, NI number, pay, email address, telephone number and images.
	Special category data	Not processed, unless otherwise specified in the Contract.
Types of data subject (e.g. staff, students)		As specified in the Contract, but may include staff (including volunteers, agents and temporary workers), customers/clients, supplier and students.
Nature and purposes of the processing		As specified in the Contract, specifically for the purposes of performing a Party's obligations under the Contract and (if applicable) pursuant to the written instructions of the Controller.
Duration of processing		For the duration contemplated in the Contract.

Part B: Definitions and Interpretation

The following words shall have the following meanings:

Commissioner means the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).

Contract means the contract between the Customer and the Supplier for the supply of services (as set out in the Customer's purchase order form), to which this DPA is supplemental.

Controller has the meaning given in section 6, DPA 2018. To the extent that a Party is deemed a Controller under the Contract, that Party shall comply with its obligations as Controller under this DPA and Data Protection Legislation.

Customer means University of York.

Data Protection Legislation means all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (DPA 2018); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the Commissioner or other relevant

	regulatory authority and which are applicable to a party.
Data Subject	means the identified or identifiable living individual to whom the Personal Data relate.
EEA	means the European Economic Area.
Personal Data	means any information relating to an identified or identifiable living individual that is processed by the Processor on behalf of the Controller as a result of, or in connection with, the provision of the services under the Contract; an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
Personal Data Breach	means a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data.
Processing, processes, processed, process	means any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third parties.
Processor	a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller. To the extent that a Party is deemed a Processor under the Contract, that Party shall comply with its obligations as Processor under this DPA and Data Protection Legislation.
Processor Personnel	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any subprocessor engaged in the performance of its obligations under a contract.
Shared Personal Data	means the Personal Data to be shared between the Parties under this DPA, as applicable.
UK GDPR	has the meaning given in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.
Supplier	has the meaning given to it in the Contract.

This DPA is subject to the terms of the Contract and is incorporated into the Contract. Interpretations and defined terms set forth in the Contract shall apply to the interpretation of this DPA. In the case of conflict or ambiguity between any provision contained in the Contract and any of the provisions of this DPA, the provisions of this DPA shall prevail.

Part C: Processing

1. Status of the Controller

1.1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under the Contract dictates the status of each party under the DPA 2018. A Party may act as:

(a) **Controller** in respect of the other Party who is **Processor**;

(b) **Joint Controller** with the other Party; or

(c) **Independent Controller** of the Personal Data where the other Party is also **Controller**.

1.2. The Controller retains control of the Personal Data and remains responsible for compliance with its obligations under the Data Protection Legislation and shall ensure that it has any required notices and consents in place to enable lawful transferring and/or Processing of the Personal Data.

2. Joint Controllers

2.1. To the extent the Parties are each deemed a Joint Controller, this clause 2 shall apply and the Parties shall comply with UK GDPR Article 26.

2.2. The parties consider this data sharing initiative necessary and proportionate for the purposes of complying with its obligations under the Contract. It is fair as it will benefit the parties by enabling them to benefit from the rights governed by the Contract and not unduly infringe the Data Subjects' fundamental rights and freedoms and interests.

2.3. Each Party shall comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Joint Controller.

2.4. The Parties agree to only Process Shared Personal Data, as described in this DPA for the purposes and by the means set out in this DPA. The Shared Personal Data must not be irrelevant or excessive with regard to such agreed purposes.

2.5. Each Party shall ensure that it Processes the Shared Personal Data fairly and lawfully in accordance with this DPA.

2.6. Each Party shall ensure that it has legitimate grounds under the Data Protection Legislation for the Processing of Shared Personal Data.

2.7. The data discloser shall ensure that Shared Personal Data is accurate and that it has appropriate internal procedures in place for the data receiver to sample Shared Personal Data and it will update the same if required prior to transferring the Shared Personal Data.

3. Independent Controllers

3.1. To the extent the Parties are deemed Independent Controllers, this clause 3 shall apply.

3.2. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party shall comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

3.3. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of the same.

3.4. Where a Party has provided Personal Data to the other Party in accordance with this DPA, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

3.5. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

3.6. The Parties shall only provide Personal Data to each other:

(a) to the extent necessary to perform their respective obligations under the Contract; and

(b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR).

3.7. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

3.8. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

4. <u>Processor's obligations</u>

4.1. To the extent a Party is deemed a Processor for the purposes of the Data Protection Legislation, this clause 3 shall apply.

4.2. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

4.3. The Processor shall only process the Personal Data to the extent, and in such a manner, as is necessary for the performance of its obligations under the Contract and in accordance with the Controller's instructions as set out in the Contract or such written instructions of the Controller as may be received in writing by the Processor from time to time.

4.4. The Processor shall not process the Personal Data for any other purpose or in a way that does not comply with this DPA, the Contract or the Data Protection Legislation.

4.5. The Processor must promptly notify the Controller in writing if, in its opinion, the Controller's instructions do not comply with the Data Protection Legislation.

4.6. The Processor must notify the Controller promptly of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting the Processor's performance of the Contract or this DPA.

4.7. The Processor must comply promptly with any Controller written instructions requiring the Processor to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

4.8. The Processor shall maintain the confidentiality of the Personal Data and shall not disclose the Personal Data to third parties unless the Controller, the Contract or this DPA specifically authorises the disclosure, or as required by the Data Protection Legislation, Court or regulator (including the Commissioner). If the Data Protection Legislation, Court or regulator (including the Commissioner) requires the Processor to process or disclose the Personal Data to a third-party, the Processor must first inform the Controller of such legal or regulatory requirement and give Controller an opportunity to object or challenge the requirement, unless the Data Protection Legislation prohibits the giving of such notice.

4.9. The Processor shall reasonably assist the Controller, at no additional cost to Controller, with meeting the Controller's compliance obligations under the Data Protection Legislation, taking into account the nature of the Processor's processing and the information available to the Processor, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commissioner or other relevant regulator under the Data Protection Legislation.

4.10. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged Processing and the purpose of the Processing;

(b) an assessment of the necessity and proportionality of the Processing in relation to the deliverables of the Contract;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

4.11. The Processor shall only collect Personal Data for the Controller using a notice or method that the Controller specifically pre-approves in writing, which contains an approved data privacy notice informing the Data Subject of the Controller's identity, the purpose or purposes for which their Personal Data shall be processed, and any other information that, having regard to the specific circumstances of the collection and expected processing, is required to enable fair processing. The Processor shall not modify or alter the notice in any way without the Controller's written consent.

5. Processor Personnel

5.1. To the extent a Party is deemed a Processor for the purposes of the Data Protection Legislation, this clause 5 shall apply.

5.2. The Processor shall ensure that all of its Processor Personnel:

(a) are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data;

(b) have undertaken training on the Data Protection Legislation and how it relates to their handling of the Personal Data and how it applies to their particular duties; and

(c) are aware both of the Processor's duties and their personal duties and obligations under the Data Protection Legislation and this DPA.

5.3. The Processor shall take reasonable steps to ensure the reliability, integrity and trustworthiness of all of its Processor Personnel with access to the Personal Data.

6. Subprocessing

6.1. For the avoidance of doubt, notwithstanding the status of the Parties, this clause 6 shall apply.

6.2. In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

6.3. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

7. Security

7.1. For the avoidance of doubt, notwithstanding the status of the Parties, this clause 7 shall apply.

7.2. The Parties must at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data. The Parties must document those measures in writing and periodically review them at least annually to ensure they remain current and complete.

7.3. The Parties must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

8. Transfers of personal data

8.1. For the avoidance of doubt, notwithstanding the status of the Parties, this clause 8 shall apply.

8.2. The Parties must not transfer or otherwise process the other Party's Personal Data outside the UK or, the EEA without obtaining that other Party's prior written consent and the following conditions are fulfilled:

(a) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37);

(b) the Data Subject has enforceable rights and effective legal remedies;

(c) each Party comply with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the other Party in meeting its obligations); and

(d) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data.

9. Complaints, data subject requests and third party rights

9.1. For the avoidance of doubt, notwithstanding the status of the Parties, this clause 9 shall apply.

9.2. Each Party must, at no additional cost to the other Party, take such technical and organisational measures as may be appropriate, and promptly provide such information to the other Party as that other Party may reasonably require, to enable them to comply with:

(a) the rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

(b) information or assessment notices served on the Controller by the Commissioner or other relevant regulator under the Data Protection Legislation.

9.3. To the extent a Party is deemed a Processor, the Processor must notify the Controller immediately in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.4. To the extent a Party is deemed a Processor, the Processor must notify the Controller within two (2) business days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

9.5. The Processor shall give the Controller, at no additional cost to the Controller, its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.6. The Processor must not disclose the Personal Data to any Data Subject or to a third party other than in accordance with the Controller's written instructions, or as required by the Data Protection Legislation.

10. Term and termination

10.1. This DPA shall remain in full force and effect so long as the Contract remains in effect or the Processor retains any of the Personal Data relating to the Contract in its possession or control.

11. Data return and destruction

11.1. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract.

11.2. The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be

retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

11.3. On the Controller's request or on termination of the Contract for any reason or expiry of its term, the Processor shall securely delete or destroy or, if directed in writing by the Controller, return and not retain, all or any of the Personal Data related to the Contract or this DPA in its possession or control.

12. Records and audit

12.1. To the extent a Party is deemed a Processor, it shall keep detailed, accurate and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, the processing purposes, categories of processing, and a general description of all technical and organisational security measures.

12.2. The Processor shall permit the Controller and its third-party representatives to audit the Processor's compliance with its DPA obligations, on at least ten (10) days' notice, during the Term. The Processor shall give the Controller and its third-party representatives all necessary assistance to conduct such audits at no additional cost to the Controller.

13. Personal Data Breach

13.1. In the event of an actual, suspected, threatened or "near miss" Personal Data Breach relating to any Personal Data shared between the Parties in respect of the Contract, the Party suffering the Personal Data Breach shall:

(a) notify the other Party promptly and in any event within 48 hours of becoming aware of a Personal Data Breach, including without limitation any event that results, or may result, in unauthorised access, loss, destruction or alteration of Personal Data in breach of this DPA. The suffering Party shall contact the other Party's main contact to notify them of the Personal Data Breach;

(b) conduct or support the other Party in conducting such investigations and analysis that the other Party reasonably requires in respect of such Personal Data Breach;

(c) implement any actions or remedial measures necessary to restore the security of compromised Personal Data;

(d) assist the other Party to make any notifications to the Commissioner and affected Data Subjects; and

(e) without undue delay and where feasible not later than 72 hours after having become aware of it notify Personal Data Breaches to the Commissioner 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.

14. Indemnification and liability

14.1. The Supplier agrees to indemnify, keep indemnified and defend at its own expense the Customer against all costs, claims, damages or expenses incurred by the Customer or for which the Customer may become liable due to any failure by the Supplier or its employees, subcontractors or agents to comply with any of its obligations under this DPA and/or the Data Protection Legislation.

14.2. Any limitation of liability of the Supplier set forth in the Contract shall not apply to this DPA's indemnity or reimbursement obligations.

14.3. For the avoidance of doubt, the limitation of liability of the Customer set forth in the Contract shall apply to this DPA.

15. Waiver

15.1. A waiver of any right or remedy is only effective if given in writing. A delay or failure to exercise, or the single or partial exercise of, any right or remedy does not waive that or any other right or remedy, nor does it prevent or restrict the further exercise of that or any other right or remedy.

16. Severance

16.1. If any provision or part-provision of this DPA is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this DPA.

17. No partnership or agency

17.1. Nothing in this DPA is intended to, or shall be deemed to, establish any partnership or joint venture between the Parties, constitute any Party the agent of the other Party, or authorise either Party to make or enter into any commitments for or on behalf of the other Party.

18. Entire agreement

18.1. This DPA constitutes the entire agreement between the Parties in relation to its subject matter and supersedes and extinguishes all previous and contemporaneous agreements, promises, assurances and understandings between them, whether written or oral, relating to its subject matter.

19. Governing law and jurisdiction

19.1. This DPA and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales. Each Party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims), arising out of or in connection with this DPA or its subject matter or formation.