THE GENERAL DATA PROTECTION REGULATION (EU 2016/679) DATA SHARING PROTOCOL

Issued by: STAFFORDSHIRE UNIVERSITY of College Road, Stoke-on-Trent, Staffordshire ST4 2DE, United Kingdom
To: *[insert name and address of data processor]*

Background Explanation

The General Data Protection Regulation (GDPR) contains extensive obligations relating to the protection of personal data by organisations operating within the European Union. It also applies to organisations outside the European Union that offer goods or services within the European Union. It applies to 'Controllers' of personal data and to 'Processors'. References to 'Personal Data', 'Controller' and 'Processor' in this Protocol shall have the same meaning as these words have in GDPR.

This Protocol sets out the basis on which we will share personal data with each other in order to fulfil our respective obligations under the agreement between us which is identified in the Schedule to this Protocol ('the Principal Agreement'). We recognise that we may be regarded in law as the Data Controller in respect of some of the data and as the Data Processor in respect of other data. In some cases, we may control the data jointly.

The Purpose and Management of the data sharing is set out in the Schedule at the end of the Protocol.

1. Undertakings of the parties

The parties acknowledge their obligations under GDPR and undertake to comply with them. In particular each party undertakes that it shall:

1.1 only process the Personal Data as necessary for the Purpose and, where it is not the Data Controller of the data, that it will only act in accordance with the Data Controller's reasonable written instructions from time to time in respect of it;

1.2 keep all Personal Data confidential and take all appropriate technical and organisational measures to ensure a level of security which is appropriate to the risks to individuals that may result from the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Personal Data. Such measures may include, as appropriate, encryption,

pseudonymisation, resilience of processing systems and the backing-up of Personal Data so that systems can be promptly reinstated;

1.3 if it receives any valid request from any person under GDPR relating to the Personal Data, provide a copy of that request to the party which is the Data Controller of that data within five working days and shall provide all reasonably necessary assistance to the Data Controller to enable it to deal with the request in accordance with GDPR;

1.4 provide promptly all reasonably necessary assistance to the Data Controller to enable it to deal with any communications from any supervisory authority (as defined in GDPR) relating to the Personal Data;

1.5 provide all reasonably necessary assistance to enable the Data Controller to comply with its obligations under GDPR including, without limitation, obligations relating to the security of personal data, the notification of breaches to any supervisory authority, the enforcement of rights by data subjects and the conduct of data protection impact assessments where required;

1.6 not transfer any Personal Data outside the European Economic Area without the prior written consent of the Data Controller

1.7 keep records of all processing of Personal Data for as long as is necessary for the Purpose or as required by law, and provide the Data Controller with a copy of those records on reasonable request;

1.8 where required by GDPR, designate a data protection officer and a representative within the European Union and provide their contact details to the Data Controller;

1.9 retain the Personal Data only for as long as is necessary for the Purpose or until its return is demanded by the Data Controller or as required by law;

1.10 not disclose the Personal Data to third parties (except to subcontractors and employees as permitted by under this Protocol) or except as instructed by the Data Controller in writing from time to time or as required by law;

1.11 ensure that access to the Personal Data is limited to those persons who need to access the Personal Data for the Purpose;

1.12 ensure that persons that may have access to the Personal Data are informed of the confidential nature of the Personal Data and have committed themselves to keeping it confidential by signing binding confidential undertakings in relation to the Personal Data, have undertaken training about GDPR, and are aware of the Data Processor's duties and their personal duties and obligations under GDPR and this Protocol;

1.13 take reasonable steps to ensure the reliability of any employees and other workers or agents who have access to the Personal Data;

1.14 not to disclose the Personal Data to any sub-contractors without the prior written consent of the Data Controller and subject to the terms of a written agreement containing measures and obligations which are broadly similar to those contained in this Protocol for the protection of the Personal Data. The Data Processor remains liable to the Data Controller for the fulfilment of obligations by any sub-contractor;

1.15 allow the Data Controller, on giving at least five working days' notice, to inspect or appoint representatives to inspect all facilities, equipment,

documents and electronic data which contain or which are used to process Personal Data by the Data Processor;

1.16 promptly remedy, at its own cost, any non-compliance with this Protocol or risks or threats reasonably identified by the Data Controller;

1.17 notify the Data Controller within 24 hours of becoming aware of any actual or suspected Personal Data breach, and provide all necessary cooperation and assistance to enable the Data Controller to investigate the breach, comply with all reporting and notification obligations under GDPR, and take all necessary and appropriate corrective action to remedy the breach, prevent a recurrence of such a breach, and avoid and/or prevent any further loss or damage arising from the breach;

1.18 notify the Data Controller forthwith if it is asked to do or to refrain from doing anything which would constitute an infringement of its obligations under GDPR or under this Protocol; and

1.19 indemnify the other party in respect of any loss or damage suffered as a result of the failure of the party in default to comply with its obligations provided the party to be indemnified promptly notifies the other party of a claim or potential claim; allows the other party to have sole control of the defence and settlement of any such claim and provides reasonable co-operation and assistance to the indemnifying party in its defence of such claim.

2. Obligations of the Data Controller

The Data Controller:

2.1 shall ensure that it is entitled to transfer and share the Personal Data with the other party for the Purpose;

2.2 is responsible for the management of any data subject requests in respect of the Personal Data it controls; and

2.3 shall comply with its obligations as a Data Controller under the GDPR

3. Consequences of Termination of the Principal Agreement

The parties shall unless otherwise required by law:

3.1.1 cease to process the Personal Data in respect of which they are not the Controller; and

3.1.2 delete or return all Personal Data to its Data Controller as requested by the Data Controller

4. Law and Jurisdiction

This Agreement is subject to English law and the jurisdiction of the English courts

SCHEDULE
The Purpose and Management of the Data Processing

- **The Principal Agreement**

Date: Parties:

- **Who are the data subjects?**

- **What data is being shared and who is the Controller of it?**

DATA	**CONTROLLER**

- **Why is the data being shared?**

- **What is the legal basis for the sharing of the data?**

E.g. Consent / Necessary for the fulfilment of a contract / Compliance with a legal obligation/ Other (please state)

- **How will the data be shared? (Specify how and when it will be transferred and security measures)**

- **How will the data be stored? (Specify any technical and organisational measures in place)**

- **Who will be responsible for the data? (Name, job title, contact details)**

- **Who will have access to the data? (Job titles)**

- **Is the data to be shared with any other organisations? (A new protocol will be needed)**

- **For how long will the data be kept?**

- **Describe the procedure for dealing with Subject Access Requests**

- **How will the data be returned to its Controller or destroyed?**

SIGNED for and on behalf of
STAFFORDSHIRE UNIVERSITY

Name:
Position:
Signature:
Date:

SIGNED for and on behalf of
[INSERT]

Name:
Position:
Signature:
Date: