



Dated

21st May

2018

TEESSIDE UNIVERSITY

And

Teesside University Students' Union

DATA SHARING AGREEMENT

Legal & Governance Services, Teesside University, Middlesbrough TS1 3BA



DATA SHARING AGREEMENT

BETWEEN

TEESSIDE UNIVERSITY (TU)

AND

TEESSIDE UNIVERSITY STUDENTS' UNION (TUSU)

BACKGROUND

- A) Teesside University ('TU') is a Higher Education Corporation established under the Education Reform Act 1988 and the Further and Higher Education Act 1992 and Teesside University Students' Union ('TUSU') is a union of TU's students that is operated as a separate legal entity with its own constitution and Board of Trustees.
- B) Although Teesside University and Teesside University Students' Union ('TUSU') are separate legal entities, TU has a legal obligation to ensure that TUSU operates in a fair and democratic manner and is accountable for its finances. TU and TUSU therefore work together in ensuring that the affairs of TUSU are properly conducted and to support the efficient delivery of services to TU students to meet their educational and welfare needs. The relationship between TU and TUSU necessarily involves the sharing of Personal Data about those students.
- C) The power that the University engages to share Personal Data with TUSU is twofold:
- a. Data is shared by virtue of the TU's duty under section 22(1) of the Education Act 1998 which states: *(1) The governing body of every establishment to which this Part applies shall take such steps as are reasonably practicable to secure that any students' union for students at the establishment operates in a fair and democratic manner and is accountable for its finances* (Article 6 (1) (e) GDPR).

Data is shared in line with TU's legitimate interests to support the efficient delivery of services by TUSU to support the educational and welfare needs of students (Article 6 (1) (f) GDPR).

- D) For the purposes of GDPR and specifically Article 6 (1) (f), TU is considered to be a hybrid authority, that is, a public authority for some, but not all of its tasks. This position is supported by the fact that TU is governed partly by a contract with its students for the delivery of educational services and partly by the principles of public law enforceable by way of judicial review.

1. DEFINITIONS

In this Agreement, the following definitions shall apply:

"Controller", "Processor" "Data Subject" and "Data Protection Officer"	shall have the meaning given to those terms in the applicable Data Protection Laws;
"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; 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; as set out in Appendix 1.
"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;
"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;
"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;
"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 (e.g. call centres) and

making ex gratia payments), all whether arising in contract, tort (including negligence), breach of statutory duty or otherwise;

"Permitted Recipients"	means the third parties to whom each Party is permitted to disclose the Personal Data, as set out in Clause 6;
"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 such Personal Data more particularly described in Appendix 1 (<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 Paragraph 3.2.2(d);
"Processing"	has the meaning set out in the Data Protection Laws (and "Process" and "Processed" shall be construed accordingly);
"Restricted Country"	means a country, territory or jurisdiction outside of 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;
"Third Party Request"	means a written request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by law or regulation; and
"TUSU objects"	means the advancement of education of TU students for the public benefit by: <ol style="list-style-type: none">Promoting the interests and welfare of students at TU during their course of study and representing, supporting and advising TU students;Being the recognised representative channel between TU and its students;Providing social, cultural, sporting and recreational activities and forums for discussion and debate for the personal development of TU students.

2. OWNERSHIP AND RESPONSIBILITIES

2.1 As TU and TUSU are separate legal entities, both are individually registered as Data Controllers with the ICO as follows:

2.1.1 Teesside University Registration Number Z5567143

2.1.2 TUSU Registration Number Z4994909

2.2 This Agreement governs the sharing of TU registered students' personal data between TU and TUSU for the purposes set out in Appendix 1 Section 3 and all sharing of student's personal data between the organisations must comply with such.

2.3 TU and TUSU are Data Controllers in common of any Personal Data shared with each other. Each organisation is separately responsible for the processing of shared Personal Data and for informing students about this processing via a Student Privacy Notice. This Agreement will be published on both TU and TUSU websites and linked from TU's Student Privacy Notice explicitly referred to in the enrolment declaration which all students are required to accept prior to enrolment/re-enrolment each academic year

3. DATA PROTECTION

3.1 Nature of the Processing

3.1.1 Each of the Parties agree that the nature of the Processing under this Agreement is as set out in Appendix 1 Section 3 and that TUSU shall be acting as a Controller when processing for this purpose.

3.1.2 Notwithstanding Paragraph 3.1.1, if either Party is deemed to be a joint Controller with the other in relation to the Personal Data, the Parties agree that they shall be jointly responsible for the compliance obligations imposed on a Controller by the Data Protection Laws, and the Parties shall cooperate to do all necessary things to enable performance of such compliance obligations, except that each Party shall be responsible, without limitation, for compliance with its data security obligations set out in Clause 7 where Personal Data has been transmitted by it, or while Personal Data is in its possession or control;

3.1.3 Each of the Parties acknowledges and agrees that Appendix 1 ("*Data Processing Particulars*") to this Agreement is an accurate description of the Data Processing Particulars.

3.1.4 Each of the Parties have jointly agreed that sharing Personal Data in accordance with this Agreement for the purposes outlined above is fair and lawful and meets the conditions of processing under Article 6 (1) (e) and 6 (1) (f) of GDPR;

3.1.5 Each of the Parties acknowledges that:

(a) the Data Protection Officer for TU is Helen Cutting, Executive Director L&GS and University Secretary h.cutting@tees 01642 384251; and

(b) the Data Protection Manager for TUSU is Jon Berg, Chief Executive TUSU J.Berg@tees.ac.uk 01642 342234.

3.2 Data Controller Obligations

- 3.2.1 Each Party shall in relation to the Processing of the Personal Data comply with its respective obligations under the Data Protection Laws.
- 3.2.2 Without limiting the generality of the obligation set out in Paragraph 3.2.1, in particular, each Party shall:
- (a) where required to do so make due notification to the ICO;
 - (b) ensure it is not subject to any prohibition or restriction which would:
 - (i) prevent or restrict it from disclosing or transferring the Personal Data to the other Party as required under this Agreement;
 - (ii) prevent or restrict it from granting the other Party access to the Personal Data as required under this Agreement; or
 - (iii) prevent or restrict either Party from Processing the Personal Data, as envisaged under this Agreement;
 - (c) ensure that all fair processing notices have been given (and/or, as applicable, consents obtained) and are sufficient in scope to enable each Party to Process the Personal Data as required in order to obtain the benefit of its rights and to fulfil its obligations under this Agreement in accordance with the Data Protection Laws.
 - (d) ensure that appropriate technical and organisational security measures are in place sufficient to comply with at least the obligations imposed on the Controller by the Security Requirements; and where requested provide to the other Party evidence of its compliance with such requirements promptly, and in any event within forty-eight (48) hours of the request;
 - (e) notify the other Party promptly, and in any event within forty-eight (48) hours of receipt of any Data Subject Request or ICO Correspondence which relates directly or indirectly to the Processing of Personal Data under, or in connection with, this Agreement and together with such notice, provide a copy of such Data Subject Request or ICO Correspondence to the other Party and reasonable details of the circumstances giving rise to it. In addition to providing the notice referred to in this Clause 3.2.2.e, each Party shall provide the other Party with all reasonable co-operation and assistance required by the other Party in relation to any such Data Subject Request or ICO Correspondence;
 - (f) use reasonable endeavours to notify the other Party if it is obliged to make a disclosure of any of the Personal Data under any statutory requirement, such notification to be made in advance of such disclosure or immediately thereafter unless prohibited by law;
 - (g) notify the other Party in writing without undue delay and, in any event, within twenty-four (24) hours of it becoming aware of any actual or suspected Personal Data Breach in relation to the Personal Data received from the other Party and shall, within such timescale to be agreed by the Parties (acting reasonably and in good faith):
 - (i) implement any measures necessary to restore the security of compromised Personal Data; and

- (ii) support the other Party to make any required notifications to the ICO and/or other equivalent relevant Regulator and affected Data Subjects;
- (h) take reasonable steps to ensure the reliability of any of its personnel who have access to the Personal Data;
- (i) not do anything which shall damage the reputation of the other Party or that Party's relationship with the Data Subjects;
- (j) not transfer any Personal Data it is processing to a Restricted Country;
- (k) hold the information contained in the Personal Data confidentially and under at least the conditions of confidence as such Party holds Personal Data Processed by it other than the Personal Data;
- (l) not disclose the Personal Data to a third party (including a sub-contractor) in any circumstances without the other Party's prior written consent, save in relation to: (i) disclosures to Permitted Recipients; and (ii) Third Party Requests. For Third Party Requests, the Party seeking to disclose the Personal Data shall use reasonable endeavours to advise the other Party in advance of such disclosure, unless that Party is prohibited by law or regulation from notifying the other Party of that disclosure, in which case it shall do so as soon as practicable thereafter (where permitted by law or regulation);and
- (m) at the other Party's option or direction, arrange for the prompt and safe return and/or secure permanent destruction of all Personal Data, together with all copies in its possession or control within 5 days and, where requested by the other Party certify that such destruction has taken place.

4. INFORMATION TO BE SHARED

- 4.1 TU will provide TUSU with the Personal Data of enrolled students as contained in Appendix 1 Section 3. In order for TUSU to fulfil its statutory obligations, Personal Data for students changing enrolment status part way during an academic year will continue to be shared with TUSU until conclusion of the academic year. Such sharing excludes any students who have opted out in accordance with Clause 10 of this Agreement.

5. INSURANCE

- 5.1 Both Parties agree:

- 5.1.1 to obtain and keep in full force and effect at all times, in respect of the Processing of the Personal Data, a policy or policies of insurance covering liability for damage arising to persons as a result of the Party's breach of this Agreement and/or failure to comply with the Data Protection Laws and which meet 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;
 - (c) it must have policy limits and provisions conforming to such requirements as the other Party may from time to time reasonably prescribe;

- 5.1.2 to deliver to the other Party upon request
- (a) copies of all applicable insurance policies taken out pursuant to the provisions of this Agreement;
 - (b) evidence of premiums paid in relation to such insurance; and
 - (c) ensure that the other Party shall be entitled to the benefit of such insurance.

6. TRANSFER TO PERMITTED RECIPIENTS

- 6.1 From the academic year 2018/2019, Membership Solutions Ltd ('UKMSL') will act as a Data Processor on behalf of TUSU. TUSU warrants that at all times it will have in force a valid written contract with UKMSL containing provisions equivalent to those set out in this data sharing Agreement and particularly provisions that comply with the requirements set out in Art 32 GDPR. TU reserves the right to withhold transfers of data where it reasonably considers that arrangements do not satisfy this requirement.
- 6.2 TU will electronically transfer Personal Data set out in Appendix 1 Section 3 to UKMSL as TUSU's Data Processor using a secure file sharing system. This transfer will ensure that TUSU hold up to date Personal Data at any given time and enable TUSU to immediately cease processing where a student opts out as per Clause 10 of this Agreement.
- 6.3 TUSU is responsible for Personal Data transferred from TU to UKMSL as if the data were directly transferred to TUSU as Data Controller. Any data breach that occurs as a result of any action/omission by TUSU, UKMSL or any third party acting on TUSU's behalf shall result in TUSU being liable in law for any consequences.
- 6.4 In the event, TUSU changes its Data Processor from UKMSL to a new supplier, TUSU and TU agree that the obligations in Clause 6.1 to 6.3 shall apply to the incoming supplier. In addition, in such an event, TUSU agrees to notify TU's DPO as specified in clause 3.1 (5) (a), immediately in writing the following:
- 6.4.1 Details of the new supplier; and
 - 6.4.2 Confirmation that clause 6.1 has been met with the new supplier

7. DATA SECURITY

- 7.1 Both TU and TUSU warrant that all Personal Data shared under this Agreement will be kept secure and protected against unauthorised access, use or disclosure. In particular, information about identifiable students will only be made accessible to individuals who require access for the purposes as specified in Clause 3.1.1.
- 7.2 If either party becomes aware of any potential data breach which involves data shared by the other, each party agrees to notify the other immediately to the contact details set out in clause 3.1.5.

8. CONDITIONS

- 8.1 With regard to the use of shared Personal Data, TUSU warrants that it will ensure:

- 8.1.1 Compliance with the Data Protection Laws.
- 8.1.2 Any employee of TUSU or its Data Processor is fully aware of the Data Protection Laws and its principles before any processing of TU student data is undertaken.
- 8.1.3 Any Data Processor used by TUSU has security policies and procedures that ensure compliance with Article 32 and Clause 7 of this Agreement.

9. RESTRICTIONS

- 9.1 Any Personal Data provided by TU to TUSU shall not be disclosed to any third party without the express written approval of TU except for the Permitted Recipients.
- 9.2 Should the data need to be released to a Data Processor to host the TUSU website, TUSU warrants that at all times it will have in force a valid written contract with the Data Processor that complies with the requirements of Art 32 GDPR and expressly prohibits the use of the data for any purpose other than that in Clause 3.1.1 and obliging the Data Processor to comply with the conditions of Clause 7 of this Agreement.
- 9.3 Any data provided by TU to TUSU shall not be used by organisations and individuals other than TUSU for the purposes of providing marketing services.
- 9.4 Information sent to students relates directly to the operational activities of TUSU or to products and services provided to TUSU, which are of genuine benefit to students.
- 9.5 TU's ITaCS department is given appropriate notification of bulk e-mails and TUSU take appropriate action in respect of any reasonable request to delay or re-schedule bulk e-mails.
- 9.6 Students are given an option in each mailing to opt out of future mailings.

10. OPT OUT RIGHTS

- 10.1 TU will ensure that all enrolling/re-enrolling students are given appropriate information about data sharing including a right to opt out of the sharing for the purposes set out in this Data Sharing Agreement. This will be communicated by way of TU's Student Privacy Notice.
- 10.2 TUSU are required to maintain a readily accessible and easy to use mechanism for students to opt out of having their Personal Data processed by TUSU at any time.
- 10.3 If a student notifies TU that they wish to opt out of their Personal Data being shared with TUSU, TU will notify TUSU and their Personal Data will no longer be included in the transfer.
- 10.4 Where a student exercises their right to opt out of SU membership, after their personal data has been shared with TUSU, TUSU will ensure that it or any Data Processors working on its behalf, destroy and cease processing any Personal Data already received without delay.

11. RETENTION

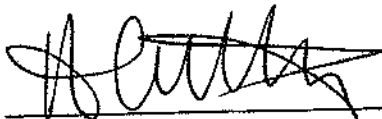
11.1 As Data Controller, TUSU is responsible for ensuring that it operates an appropriate data retention policy and shall ensure that any Personal Data transferred under this Agreement is not kept for longer than is necessary to perform the processing for which it was collected as per Clause 4 of this Agreement.

12. REVIEW

12.1 This Agreement is to be reviewed annually to ensure that it continues to reflect the requirements of Data Protection Laws the purposes remain valid and ensure fairness to students. If no changes are required, it may be re-confirmed by e-mail. In exceptional circumstances where urgent and necessary changes are required, an additional review may occur.

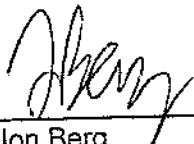
12.2 TUSU acknowledge that TU may suspend and/or terminate the provision of data at any time, with or without notice, where the TU acting reasonably considers that the safeguards for Personal Data are not adequate or adequately implemented to protect the individual rights of its students.

12.3 Nothing in this Agreement will limit or restrict either TU or TUSU's obligation to ensure compliance with the Data Protection Laws in relation to data where they are the Data Controller.



Helen Cutting
University Secretary, Teesside University

Date: 21 May 2018



Mr Jon Berg
Chief Executive, Teesside University Students' Union

Appendix 1

Data Protection Particulars

Section 1. The subject matter and duration of the Processing	<p>Although Teesside University ('TU') and Teesside University Students' Union ('TUSU') are separate legal entities, TU has a legal obligation to ensure that TUSU operates in a fair and democratic manner and is accountable for its finances. TU and TUSU therefore work together in ensuring that the affairs of TUSU are properly conducted and to support the efficient delivery of services to TU students to meet their educational and welfare needs. The relationship between TU and TUSU necessarily involves the sharing of Personal Data about those students.</p> <p>In respect of the power that the University engages to share Personal Data with TUSU this is twofold:</p> <ol style="list-style-type: none">1. Data is shared by virtue of the TU's duty under section 22(1) of the Education Act 1998 which states: <i>(1) The governing body of every establishment to which this Part applies shall take such steps as are reasonably practicable to secure that any students' union for students at the establishment operates in a fair and democratic manner and is accountable for its finances</i> (Article 6(1) (e) GDPR).2. Additionally, the sharing is in line with TU legitimate interests to support the efficient delivery of services by TUSU to support the educational and welfare needs of students (Article 6 (1) (f) GDPR) for the duration of their studies. <p>For the purposes of GDPR and specifically Article 6 (1) (f), TU is considered to be a hybrid authority, that is, a public authority for some, but not all of its tasks. This position is supported by the fact that TU is governed partly by a contract with its students for the delivery of educational services and partly by the principles of public law enforceable by way of judicial review.</p>
Section 2. The nature and purpose of the Processing	<p>TUSU objects are the advancement of education of TU students for the public benefit by:</p> <ol style="list-style-type: none">1. promoting the interests and welfare of students at TU during their course of study and representing, supporting and advising TU students.2. being the recognised representative channel between TU and its students.3. providing social, cultural, sporting and recreational activities and forums for discussion and debate for the personal development of TU students. <p>To support TUSU in meeting its objects, TUSU requires access to the Personal Data of TU students detailed at in the next section of this Appendix, to be used by TUSU for the following purposes</p>

	<ol style="list-style-type: none"> 1. Administration of TUSU elections. 2. Administration of TUSU clubs, societies and other student opportunities. 3. Maintenance of TUSU membership requirements. 4. Generation of demographic reports including demographic analysis of TUSU service use/event participation. 5. To understand and develop the academic impact of student engagement with TUSU. 6. Verification of student's identity. 7. Administration of ticket sales. 8. Monitoring students' entitlements to TUSU services, events or facilities that are dependent on status or number of credits studied. 9. To allow e-mail communication between TUSU and its members. 10. To allow e-mail communication between TUSU clubs & societies members where no e-mails are visible to the sender. <p>and also for the non-routine processing of Personal Data as follows:</p> <ol style="list-style-type: none"> 11. To allow TUSU and TU to collaborate on academic and welfare casework issues relating to TU students, where students are receiving casework support from TUSU. In these circumstances specific consent will be obtained from the student prior to sharing; 12. To advise of any student disciplinary issues which may impact a student's status; 13. To allow TUSU to manage, appoint and coordinate the election and engagement of TU student course representatives and deliver any required training. Name, student number, school, course, year of study and e-mail address will be shared between TUSU and TU via e-mail.
<p>Section 3. The type of Personal Data being Processed</p>	<p>TU will provide TUSU with the following Personal Data for enrolled students. In order for TUSU to fulfil its statutory obligations, Personal Data for students changing enrolment status part way during an academic year will continue to be shared with TUSU until conclusion of the academic year. Such sharing excludes any students who have opted out in accordance with Clause 10 of this Agreement.</p> <ol style="list-style-type: none"> 1. Student ID number 2. Library ID number 3. TU e-mail address

<p>Section 4. The categories of Data Subjects</p>	<ol style="list-style-type: none"> 4. Forename, middle name, surname, known as name 5. Home & term-time addresses including date of last update. 6. Date of birth 7. Age on entry 8. Gender 9. Nationality 10. Domicile 11. Programme of study 12. Course Level 13. Mode of study 14. Location of study 15. Year of study 16. Fee status 17. Major Source of Funding 18. Academic School 19. Enrolment status 20. New entrant flag <p>TUSU may provide TU with the Student ID number of groups of its members. This is strictly for the purpose of performing anonymised statistical analysis for TUSU in accordance with section 2 of this Appendix.</p> <p>No Sensitive Personal Data will be transferred between TU and TUSU.</p>
	<p>Students of TU</p>

