Schedule 4

DATA PROTECTION

1. **DEFINITIONS**

In this Schedule 4 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"	The EU General Data Protection Regulation 2016/679 ("GDPR") and Directive 2002/58/EC (ePrivacy Directive), as transposed into domestic legislation of each member state of the EU and as amended, replaced, or superseded from time to time ("EU Data Protection Laws"); The Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426, any other applicable UK laws relating to the Processing of Personal Data or privacy including any code of practice or guidance issued by the ICO, as amended, replaced, or superseded from time to time ("UK Data Protection Laws"); and Insofar as either Party is subject thereto, any other applicable data protection or privacy laws and regulations, including but not limited to any EU, member state, international, or otherwise applicable laws and regulations, and any amendments or successors thereto
"**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 Annex 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;
Permitted Recipients"	means the third parties to whom each Party is permitted to disclose the Personal Data, as set out in more detail in Annex 1 (*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 Annex 1 (*Data Processing Particulars*));
"Personal Data Breach"	has the meaning set out in the Data Protection Laws and for the avoidance of doubt , includes a breach of Paragraph 2.2.2(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.

2. DATA PROTECTION

2.1 Nature of the Processing

2.1.1 The Parties acknowledge that the factual arrangements between them dictate the role of each Party in respect of the Data Protection Laws. Notwithstanding the foregoing, each Party agrees that the nature of the Processing under this Agreement will be as follows:

(a) the Parties shall each Process the Personal Data;

(b) each Party shall be a Controller of the Personal Data acting individually and in common;

(c) Notwithstanding Paragraph 2.1.1(b), 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 Paragraph 2.2.2(d) where Personal Data has been transmitted by it, or while Personal Data is in its possession or control.

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

2.2 **Data Controller Obligations**

2.2.1 Each Party shall in relation to the Processing of the Personal Data comply with its respective obligations under the Data Protection Laws.

2.2.2 Without limiting the generality of the obligation set out in Paragraph 2.2.1, 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 privacy 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;

(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 Paragraph 2.2.2(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 relevant regulatory body 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; 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;

Annex 1

Data Protection Particulars

The subject matter and duration of the Processing	The EPSRC Centre for Doctoral Training in Renewable Energy Northeast Universities (ReNU) is an added value doctoral training programme funded by the Engineering and Physical Sciences Research Council. ReNU awards individual doctoral studentships which include a stipend and payment of tuition fees, and research training support grant (RTSG) to support activities associated with primary research, such as consumables, fieldwork and data collection; participation in specialist training and outreach events, attendance to conferences and workshops; and placements in partner organisations (from higher education institutions (HE) and non-HE). In order to run a rigorous studentship competition and manage studentships across a partnership encompassing three Universities, ReNU management committee (ReNU MC) processes personal data. EPSRC funding for ReNU is from 1st April 2019 to 30 September 2027, subject to continuation or extension by EPSRC.
The nature and purpose of the Processing	Data is held by the individual institutions and shared between them for the purpose of statutory reporting, training individual doctoral candidates, coordinating supporting physical and human resources (facilities, supervisors, collaborators, etc), and enabling the research of individual projects.
The type of Personal Data being Processed	Personal Data • Biographical (Name, Date of birth, Gender Identity) • Personal contact details • Professional contact details • Employment Details • Degree & Qualification • Nationality • University ID. • Application Details • Marital Status • Academic Progression • Disciplinary Special Category Data • Health (Disability, sickness absence) • Race (EPSRC uses the term Ethnicity) • Religion • Sex Orientation
The categories of Data Subjects	• Applicants and Enquirers • Enrolled Students • Staff • Aligned students • Project Partners