INTO UNIVERSITY PARTNERSHIPS LIMITED

APPROPRIATE POLICY DOCUMENT: SPECIAL CATEGORY AND CRIMINAL OFFENCE DATA

1. In the course of our business, we need to process both Special Category ("**SC**") data and Criminal Offence ("**CO**") data. When we undertake such processing we comply with the General Data Protection Regulation (the "**GDPR**") and the Data Protection Act 2018 (the "**DPA**") as well as any further laws, codes of practice or guidance in relation to processing personal data and privacy which are either enacted or published by a relevant supervisory authority and which are applicable to us from time to time.

2. Specifically, our processing of SC and CO data complies with Articles 9 and 10 of the GDPR, Schedule 1 of the DPA, and the data protection principles set out in the GDPR. The purpose of this policy document is to explain how our processing of this kind of data is consistent, where applicable, with these articles, conditions and principles, as well as to tell you about the length of time we need to hold such data.

3. WHAT IS SC DATA?

3.1 Article 9 of the GDPR defines SC data as being personal data which includes or reveals:

3.1.1 Racial or ethnic origin;

3.1.2 Political opinions;

3.1.3 Religious or philosophical beliefs;

3.1.4 Trade union membership;

3.1.5 Genetic data;

3.1.6 Biometric data for the purpose of uniquely identifying a natural person;

3.1.7 Data concerning health; and

3.1.8 Data concerning a natural person's sex life or sexual orientation.

3.2 Article 10 of the GDPR covers the processing of personal data which relates to criminal convictions, criminal offences, or related security measures.

3.3 Data protection law says that we can only process SC data if one of the conditions in Article 9(2) GDPR and/or in Schedule 1 of the DPA applies. If we process CO data, then this too must be on the basis of one of the Schedule 1 conditions.

3.4 Most of the conditions for processing SC or CO data also require us to have this document in place (an "Appropriate Policy Document") which explains our procedures for compliance, and for the retention and erasure of the data.

4. DESCRIPTION OF THE DATA WE PROCESS

4.1 We process special category data about our employees, prospective employees and former employees, including medical data, data in relation to physical or mental health, passport details and details in relation to equal opportunities monitoring. In each case, we process this data because it is necessary for us to fulfil our obligations or exercise our rights as an employer.

4.2 We process CO data about our employees, prospective employees and former employees as a part of our background checks, or where we need to comply with a legal obligation.

4.3 We also process SC and CO data about our students and prospective students including medical data, data in relation to disabilities, physical or mental health, details in relation to equal opportunities monitoring and criminal convictions.

5. SCHEDULE 1 CONDITIONS

5.1 We rely on the following Schedule 1 conditions when we process SC data:

5.2 **Part 1, Schedule 1 – Employment, Health and Research etc**

5.2.1 **Paragraph 1(1)(a)** employment, social security and social protection.

Processing includes:

(a) employee health data, and the passport details of prospective employees in accordance with the above condition when we manage business travel and in connection with employee familiarisation trips;

(b) medical data, physical or mental health data and ethnicity data in accordance with the above condition to create and maintain a personnel file;

(c) health data in accordance with the above condition to determine absences from work in the context of payroll requirements, and for pension administration.

5.3 **Part 2, Schedule 1 – Substantial Public Interest Conditions**

5.3.1 **Paragraph 6(1)** and **(2)(a)** statutory, etc. purposes

Processing includes

(a) ethnicity data and other SC data in accordance with the above condition where we are required to monitor equality of opportunity;

(b) student and prospective student disability data in accordance with the above condition to ensure that we can make reasonable adjustments necessary to ensure equality of access to student accommodation;

(c) student and prospective student ethnicity data in accordance with the above condition in relation to compliance with visa conditions.

5.3.2 **Paragraph 8(1)** equality of opportunity or treatment.

5.3.3 **Paragraph 10(1)** preventing or detecting unlawful acts.

5.3.4 **Paragraph 18(1)** safeguarding of children and of individuals at risk.

5.4 We only process CO data where such processing is consistent with the following purposes in Parts 1 and 2 of Schedule 1:

5.4.1 **Paragraph 1(1)(a**) employment, social security and social protection.

(a) criminal conviction data in accordance with the above condition when we recruit employees.

5.4.2 **Paragraph 6(1)** and **6(2)(a)** statutory, etc. purposes.

(a) criminal conviction data to comply with our obligations under immigration law.

5.4.3 **Paragraph 10(1)** preventing or detecting unlawful acts.

6. PROCEDURES FOR COMPLYING WITH THE PRINCIPLES

6.1 The GDPR sets out a number of principles in relation to the processing of personal data. These are set out below, together with measures we have taken to ensure that our processing of SC and CO data is in compliance with them.

6.2 **Accountability**

6.2.1 The GDPR requires us not only to comply with the data protection principles set out below, but to be able to demonstrate that we comply with them.

6.2.2 We have adopted several measures to meet this accountability requirement, including:

(a) appointing a Data Protection Officer to oversee our compliance and to ensure that data protection is at the heart of our decision making;

(b) implementing and maintaining an accurate record of our processing activities;

(c) implementing technical and organisational measures to protect the personal data that we process;

(d) putting a process in place to ensure that appropriate agreements are in place with organisations with whom we share personal data;

(e) ensuring we have appropriate privacy policies in place, and that our processing is consistent with them; and

(f) carrying out, where necessary, data privacy impact assessments.

6.3 **Principle (a): processing must be lawful, fair and transparent**

6.3.1 GDPR states that processing must be lawful, fair and transparent. For processing to be lawful, it must be specifically consented to by the data subject, or be necessary for one of the reasons set out in Article 6 of the GDPR. If the processing relates to SC or CO data, one of the Schedule 1 conditions must also apply.

6.3.2 We have identified a lawful basis for our processing, and a further Schedule 1 condition where the processing involves SC or CO data.

6.3.3 We set out our lawful bases for our processing (and the further conditions on which we rely) in our privacy notices, in greater detail in our Record of Processing Activity, and in this document. Our privacy notices provide transparent information about our processing.

6.3.4 We only process personal data in ways people would reasonably expect and use data privacy impact assessments and legitimate interests assessments to ensure that our processing is fair.

6.3.5 We are open and honest when we collect SC or CO data and do not mislead people about how we use it.

6.4 **Principle (b): personal data must be collected for specific and legitimate purposes and processed in accordance with those purposes**

6.4.1 Our privacy notices explain the purposes for which we process personal data, and we do not process personal data for purposes other than these.

6.4.2 We process SC data and CO data only where it is necessary for the purposes set out in one of the Schedule 1 conditions.

6.4.3 We do not process personal data for purposes which are incompatible with the purposes for which they were originally collected (unless this is to comply with a legal obligation, or to exercise a function which is set out in law).

6.5 **Principle (c): personal data must be adequate, relevant and limited to what is necessary for the stated purposes**

6.5.1 We aim to ensure we have sufficient SC and CO data for the purposes set out in the Schedule 1 conditions above, but do not collect or otherwise process SC or CO data in excess of what we require for these purposes.

6.5.2 If the DPO becomes aware that personal data is provided to us which is not relevant for our purposes, we will require employees to erase it.

6.5.3 We use national guidance and take external advice to help us determine what information we need to process.

6.6 **Principle (d): personal data must be accurate and, where necessary, kept up-to-date**

6.6.1 We have processes in place to check the accuracy of the SC and CO data we hold, and we record the source of such data.

6.6.2 We correct any inaccuracies in the SC and CO data we hold when data subjects exercise their rights under Article 16.

6.6.3 We keep a record of any challenges to the accuracy of the personal data we hold.

6.7 **Principle (e): personal data must be retained for no longer than necessary**

6.7.1 We are considering how long we need to process the SC and CO data for to enable us to justify the retention period we decide upon.

6.7.2 As part of our Data Retention Policy and Schedule, we will implement reviews of the SC and CO data we hold and seek to erase it when it is no longer necessary for the purposes for which it was collected.

6.8 **Principle (f): personal data must be kept securely**

6.8.1 We use encryption and pseudonymisation where we consider it appropriate for the level of sensitivity of the SC or CO data that we are processing.

6.8.2 We have, and have implemented, an information security policy.

6.8.3 We train our employees in the secure handling of SC and CO data in particular, and personal data in general.

6.8.4 We limit access to personal data to those of our employees, agents, contractors and third parties to those who have a business need to know the information.

6.8.5 We ensure that organisations that process personal data on our behalf implement technical and organisational measures which are sufficient to ensure the security of the data being processed.

7. RETENTION AND ERASURE

7.1 As set out above, we aim to retain personal data only for as long as necessary to fulfil the purposes we collected it for, including satisfying any legal, accounting, or reporting requirements (for example, to comply with reporting requirements in relation to UK Visas and Immigration, or tax reporting requirements to HMRC). We may also retain personal data for a period after this time if it is necessary and relevant for our legitimate operations.

7.2 In some circumstances we may anonymise personal data (so that it can no longer be associated with an individual) for statistical purposes, in which case we may use this information indefinitely.

7.3 Once an employee, worker or contractor leaves the company we will retain or destroy SC or CO data in accordance with applicable laws and regulation.

7.4 Our retention and erasure procedures are further documented in our Data Retention Policy & Schedule.

8. REVIEW DATE

8.1 This Appropriate Policy Document will be reviewed annually.