

## **1. CONSIDERATION**

In consideration of each of the parties entering into this Agreement (such consideration being agreed by the parties to be good and valuable consideration, the adequacy and sufficiency of which is hereby acknowledged and agreed), the parties have agreed to vary the Original Contract in accordance with Clause 17.

## **2. VARIATION OF THE ORIGINAL CONTRACT**

- 2.1 The parties agree with effect from the date of this Agreement the Original Contract shall be varied as set out in Annex 1 attached.
- 2.2 Subject to the variations set out in Annex 1, the Original Contract shall continue in full force and effect in all respects.
- 2.3 In addition to the amendments set out in Annex 1, the Original Contract shall be construed and interpreted with such further consequential amendments as are necessary to give effect to the amendments set out in Annex 1 of this Agreement, as if such further amendments were also expressly set out in Annex 1.
- 2.4 Except as provided in Clause 2.3 and Annex 1, the parties agree that no other liabilities, financial or otherwise, shall accrue to the Department because of this Variation Agreement.

## **3. SEVERABILITY**

The provisions of this Agreement are intended by the parties to be severable in the event that any part of it is held to be illegal or unenforceable (in whole or in part) and such part shall not affect the validity and enforceability of the remaining provisions or the remainder of the affected provision under this Agreement.

## **4. AUTHORITY AND COSTS**

Each party undertakes that it has full power and authority to enter into and shall be responsible for its own costs arising in relation to this Agreement.

## **5. THE CONTRACTS (RIGHTS OF THIRD PARTIES) ACT 1999**

- 5.1 Subject to Clause 5.2 below, this Agreement is not intended to create any benefit, claim or rights of any kind whatsoever enforceable by any person who is not a party to this Agreement. Accordingly, the parties confirm that no term of this Agreement is enforceable under the Contracts (Rights of Third Parties) Act 1999 by a person who is not a party to this Agreement.
- 5.2 It is the intention of the parties that any other department, officer or agency of the Crown, may as required from time to time act as the Department's agent in enforcing the Department's rights under this Agreement.

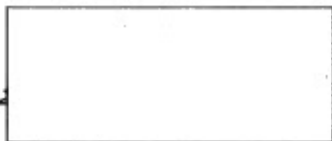
## **6. GOVERNING LAW AND JURISDICTION**

The parties agree that this Agreement and any dispute arising under or in any way connected with the subject matter of this Agreement (whether of a contractual or tortious nature or otherwise) shall be governed by and construed in accordance with the laws of England, and the parties submit to the jurisdiction of the English Courts.

**EXECUTED** by the parties on the first date in this Agreement.

**Authorised to sign for and on behalf of  
the Secretary of State for Education**

Signature



Date

18/05/18

Name in Capitals



Address in full

Department for Education  
Sanctuary Buildings  
Great Smith Street  
London  
SW1P 3BT

**Authorised to sign for and on behalf of  
IFF Research**

Signature



Date 15/5/2018

Name in Capitals



Address in full

IFF Research  
5<sup>th</sup> floor, St Magnus House  
3 Lower Thames Street  
London  
EC3R 6HD

## ANNEX 1

### VARIATIONS TO ORIGINAL CONTRACT

All references to Clauses in this Annex 1 are to Clauses in the Original Contract.

- 1 Clause 7 including Definitions shall be amended in its entirety to read as below:
- 2 A new **Schedule 4 Processing, Personal Data and Data Subjects** shall be inserted.

#### Data Protection

"Controller", "Processor," "Data Subject", "Personal Data", "Personal Data Breach", "Data Protection Officer"	take the meaning given in the GDPR
"Data Loss Event"	any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach.
"DPA 2018"	Data Protection Act 2018
"Data Protection Impact Assessment"	an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.
"Data Protection Legislation"	(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy;
"Data Subject Access Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.
"GDPR"	the General Data Protection Regulation (Regulation (EU) 2016/679)
"LED"	Law Enforcement Directive (Directive (EU) 2016/680)
"Protective Measures"	appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an

incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it.

"Sub-processor"

any third Party appointed to process Personal Data on behalf of the Contractor related to this Contract

## **7 Data Protection**

7.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Department is the Controller and the Contractor is the Processor. The only processing that the Contractor is authorised to do is listed in Schedule 4 by the Department and may not be determined by the Contractor.

7.2 The Contractor shall notify the Department immediately if it considers that any of the Department's instructions infringe the Data Protection Legislation.

7.3 The Contractor shall provide all reasonable assistance to the Department in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Department, include:

- (a) a systematic description of the envisaged processing operations and the purpose of the processing;
- (b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;
- (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.

7.4 The Contractor shall, in relation to any Personal Data processed in connection with its obligations under this Contract:

- (a) process that Personal Data only in accordance with Schedule 4, unless the Contractor is required to do otherwise by Law. If it is so required the Contractor shall promptly notify the Department before processing the Personal Data unless prohibited by Law;
- (b) ensure that it has in place Protective Measures, which have been reviewed and approved by the Department as appropriate to protect against a Data Loss Event having taken account of the:

- (i) nature of the data to be protected;
- (ii) harm that might result from a Data Loss Event;
- (iii) state of technological development; and
- (iv) cost of implementing any measures;

(c) ensure that :

- (i) the Contractor Personnel do not process Personal Data except in accordance with this Contract (and in particular Schedule 4);
- (ii) it takes all reasonable steps to ensure the reliability and integrity of any Contractor Personnel who have access to the Personal Data and ensure that they:
  - (A) are aware of and comply with the Contractor's duties under this clause;
  - (B) are subject to appropriate confidentiality undertakings with the Contractor or any Sub-processor;

- (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Department or as otherwise permitted by this Contract; and
  - (D) have undergone adequate training in the use, care, protection and handling of Personal Data; and
- (d) not transfer Personal Data outside of the EU unless the prior written consent of the Department has been obtained and the following conditions are fulfilled:
  - (i) the Department or the Contractor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Department;
  - (ii) the Data Subject has enforceable rights and effective legal remedies;
  - (iii) the Contractor complies 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 Department in meeting its obligations); and
  - (iv) the Contractor complies with any reasonable instructions notified to it in advance by the Department with respect to the processing of the Personal Data;
- (e) at the written direction of the Department, delete or return Personal Data (and any copies of it) to the Department on termination of the Contract unless the Contractor is required by Law to retain the Personal Data.

7.5 Subject to clause 7.6, the Contractor shall notify the Department immediately if it:

- (a) receives a Data Subject Access Request (or purported Data Subject Access Request);
- (b) receives a request to rectify, block or erase any Personal Data;
- (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
- (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;
- (e) receives a 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
- (f) becomes aware of a Data Loss Event.

7.6 The Contractor's obligation to notify under clause 7.5 shall include the provision of further information to the Department in phases, as details become available.

7.7 Taking into account the nature of the processing, the Contractor shall provide the Department with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 7.5 (and insofar as possible within the timescales reasonably required by the Department) including by promptly providing:

- (a) the Department with full details and copies of the complaint, communication or request;
- (b) such assistance as is reasonably requested by the Department to enable the Department to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
- (c) the Department, at its request, with any Personal Data it holds in relation to a Data Subject;
- (d) assistance as requested by the Department following any Data Loss Event;

- (e) assistance as requested by the Department with respect to any request from the Information Commissioner's Office, or any consultation by the Department with the Information Commissioner's Office.
- 7.8 The Contractor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Contractor employs fewer than 250 staff, unless:
  - (a) the Department determines that the processing is not occasional;
  - (b) the Department determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
  - (c) the Department determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.
- 7.9 The Contractor shall allow for audits of its Data Processing activity by the Department or the Department's designated auditor.
- 7.10 The Contractor shall designate a data protection officer if required by the Data Protection Legislation.
- 7.11 Before allowing any Sub-processor to process any Personal Data related to this Contract, the Contractor must:
  - (a) notify the Department in writing of the intended Sub-processor and processing;
  - (b) obtain the written consent of the Department;
  - (c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause such that they apply to the Sub-processor; and
  - (d) provide the Department with such information regarding the Sub-processor as the Department may reasonably require.
- 7.12 The Contractor shall remain fully liable for all acts or omissions of any Sub-processor.
- 7.13 The Contractor may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Contract).
- 7.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Department may on not less than 30 Working Days' notice to the Contractor amend this Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

#### **Schedule 4 Processing, Personal Data and Data Subjects**

The Contractor shall comply with any further written instructions with respect to processing by the Department.

Any such further instructions shall be incorporated into this Schedule.

Description	Details
Subject matter of the processing	The survey will explore disabled students' awareness and understanding of DSA and their experiences of applying for and receiving DSA and other forms of learning support. It will assess the impacts of DSA (and other forms of teaching and learning support) on their decision to enter HE and on their course experience.
Duration of the processing	<p>The student research will start with an online survey in late May-June 2018 followed by qualitative depth interviews among a sample of students who agree to be re-contacted for this purpose, in June-July.</p> <p>Data will continue to be processed during the analysis phase over the remainder of summer 2018 but this will be on an anonymised basis (ie no individual names or contact details will be stored with the data being analysed).</p>
Nature and purposes of the processing	<p>IFF Research will not be receiving any personal data (eg student contact details) directly from higher education institutions as they will send the survey link to relevant students on our behalf. We will only collect names and contact details of those students who agree to be recontacted for the follow-up qualitative stage of the research, and these will be stored separately from the survey information that we collect and destroyed after use, once the qualitative interviews have completed.</p> <p>The survey data will therefore be analysed on an anonymised basis ie. it will not contain any personal contact details.</p> <p>The purpose of the data collection and processing is for research purposes, in order to assess the operation and impact of DSA among higher education students, with a view to identifying any improvements.</p>
Type of Personal Data	<p>As noted above, IFF will not be receiving any identifiable personal detail (eg, names, contact details) unless a student who completes the survey actively agrees to being re-contacted for the follow-up qualitative research.</p> <p>If this is the case, we will ask them for their name, telephone number(s) and email address, which will be linked to the survey information through the use of a unique identifier (to enable us to 'target' different types of student in the qualitative research, for inclusiveness and to ensure we cover a breadth of experience). These contact details will be stored securely and separately from the survey data and will be destroyed once the qualitative fieldwork stage is complete.</p>



Categories of Data Subject	Higher education students with a declared disability who are either receiving DSA or not receiving DSA
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	<p>How long the Contractor will keep data is separated into two categories.</p> <p>CONFIDENTIAL (stored in regular Job folders) and RESTRICTED (stored in Secure Files job folders) which includes any files containing personally identifiable information such as names and contact details.</p> <p>Data retention is governed by this classification. Confidential data is included as part of the Contractor's general Business Continuity procedures by way of daily incremental backups (backups are encrypted in transit and at rest). A backup period covers one calendar month after which a new backup set will be established. The previous backup sets will be retained for 12 months, for archival purposes and for potential data recovery requests which extend beyond a previous months archives. All data backups are fully indexed. Maintaining file, file contents search capability via backup application interface. Backups are accessible only by the Contractor's IT administrative staff, with access governed by the Associate Director of IT.</p> <p>Restricted data backups are handled separately to general Business Continuity procedures. Broadly speaking similar processes surround the backup processes. The backups are accessible only by the Associate Director of IT and data recovery procedures are subject to restricted data access controls (with data controller authority) as detailed below.</p> <p>RESTRICTED data is stored encrypted, in a restricted area of the Contractor's system and subject to access controls. A data controller (Research Manager) manages access rights based on the principle of least privilege, with access right grants and revokes on demand. The entire process of restricted data access is in addition to controls, audited down to file level for who did what and when. CONFIDENTIAL data is accessible only via authorised logon accounts.</p> <p>Data destruction principals follow guidelines issued via DoD 5220.22-M. Depending on the task at hand (determined by the granularity of the data in question) two data sanitisation applications will be employed. Microsoft SDELETE (for file level deletion demands) and Active@ ZDelete for broader (folder\sub-folder or volume) deletion demands.</p> <p>Any survey data transferred to the Department / the Data Archive will be anonymised beforehand and transferred using our secure FTP site. We will check the data to ensure that there are no combinations of individual characteristics which might enable a student to be identified, for example by removing any institutional identifiers and by only including ranges rather than specific values in terms of the amount of DSA awarded.</p>

