Joint Schedule 11 (Processing Data)

Definitions

1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Processor Personnel"	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;

Status of the Controller

2. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

(a) "Controller" in respect of the other Party who is "Processor";

(b) "Processor" in respect of the other Party who is "Controller";

(c) "Joint Controller" with the other Party;

(d) "Independent Controller" of the Personal Data where the other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 (Processing Personal Data) which scenario they think shall apply in each situation

Where one Party is Controller and the other Party its Processor

3. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.

4. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

5. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged Processing and the purpose of the Processing;

(b) an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;

(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.

6. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

(a) Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms*,* which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;

(B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

(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 Controller or as otherwise permitted by the Contract; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data;

(d) not transfer Personal Data outside of the UK or EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(i) the Controller or the Processor has provided appropriate

safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Processor 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 Controller in meeting its obligations); and

(iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

(e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

7. Subject to paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract 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 the 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 Personal Data Breach.

8. The Processor's obligation to notify under paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.

9. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 7 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

(a) the Controller with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Controller following any Personal Data Breach; and/or

(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

10. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

(a) the Controller determines that the Processing is not occasional;

(b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

(c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

11. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

12. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

13. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:

(a) notify the Controller in writing of the intended Subprocessor and Processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and

(d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

14. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

15. The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 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 the Contract).

16. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Where the Parties are Joint Controllers of Personal Data

17. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11.

Independent Controllers of Personal Data

18. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

19. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

20. Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

21. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

22. The Parties shall only provide Personal Data to each other:

(a) to the extent necessary to perform their respective obligations under the Contract;

(b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and

(c) where it has recorded it in Annex 1 *(Processing Personal Data).*

23. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the

requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

24. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

25. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **("Request Recipient")**:

(a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

(b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

(i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

(ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

26. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:

(a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

(b) implement any measures necessary to restore the security of any compromised Personal Data;

(c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

(d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

27. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1

(Processing Personal Data).

28. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.

29. Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 18 to 28 of this Joint Schedule 11.

30. Special Terms – This section gives further enhanced clarity on the specifics of this agreement.

(a) INTERPRETATION

The following definitions and rules of interpretation apply to Clause 30: Special Terms.

(i) Definitions

Commencement Date	has the meaning given in Special Terms Schedule 1, Table 2.
Destroy	means safely and permanently destroy all hard and electronic copies of the Personal Data processed by the Supplier for the Permitted Use from all computers, file or document management systems and networks within the control of the Supplier, including backups. **Destroyed** shall be construed accordingly.
DfE Data	any information contained within or derived from DfE databases as more particularly described in Recital A.
DfE Processed Data Extracts	the data extracts created by DfE from the DfE Data (but not the Matched Dataset).
DSAP	means DfE's Data Sharing Approval Panel.
Identifiers	Any data classed as identification level 1 (instant identifiers including name, full address, email address) and/or identification level 2 (meaningful identifiers such as Unique Pupil Number) in accordance with the DfE safe data framework published on GOV.UK.

Licence End Date:	the end date of this agreement as specified in Special Terms Schedule 1, Table 2.
Mandatory Clauses	the mandatory clauses required by Article 28(3) of the retained version of the EU law version of the General Data Protection Regulation ((EU) 2016/679) for contracts between Controllers and Processors as those clauses are set out in the Agreement.
Matched Dataset	the matched dataset created by DfE as a result of DfE undertaking a Matching Request. **Matched Datasets** shall be construed accordingly.
Matching Request	a request received by DfE to match DfE Data with third party data.
Permitted Intended Outputs	the intended output of the processing of the Personal Data by the Supplier as required by DfE and as more particularly described in Special Terms Schedule 1, Table 2.
Permitted Use	the processing of the Personal Data as permitted by DfE to enable the Supplier to produce the Permitted Intended Outputs.
Personal Data	means any of the: (I) DfE Data Extracts; and/or (II) Matched Dataset, which contains information relating to an identified or identifiable living individual that is processed by the Supplier on behalf of DfE as a result of or in connection with the provision of the services under the Agreement.
Termination Date	the Licence End Date or such earlier date as this agreement is terminated in accordance with Clause 7.

(ii) This Clause 30 is subject to the terms of the Agreement and is incorporated into the Agreement. Except as set out herein, the interpretation and defined terms set forth in the Agreement shall apply to the interpretation of this Clause 30.

(iii) The Schedules form part of this Clause 30 and shall have effect as if set out in full in the body of this Clause 30. Any reference to

this Clause 30 includes its Schedules.

(b) CONSIDERATION

Where the Supplier processes Personal Data for DfE (as a Controller) pursuant to the services the Supplier is providing to DfE under the Agreement, DfE requires additional terms and conditions to apply to that processing and, in consideration of the exchange of mutual promises between the parties under this Clause 30 and the payment of the sum of £1 (receipt of which the Supplier expressly acknowledges), DfE and the Supplier agree that the terms and conditions set out in this Clause 30 shall apply to the processing of the Personal Data by the Supplier under the Agreement.

(c) COMMENCEMENT AND DURATION

(i) This Clause 30 shall commence with effect from the Commencement Date and shall end on the Termination Date.

(ii) The content of this Clause 30 shall be reviewed by the Parties annually (as a minimum) and must be revisited by the Parties 30 working days prior to the Licence End Date in respect of the processing of the DfE Data Extracts and/or Matched Datasets (as applicable). Where required by DfE, the Supplier shall enter into a variation to this Clause 30 (as more particularly described in Clause **Error! Reference source not found.** to this Clause 30) or enter into an agreement with DfE upon such terms and conditions as DfE may reasonably require.

(iii) The Parties agree that this Clause 30 shall supersede and replace any previous agreements relating to the Agreement and entered into between the Parties in respect of the processing of the DfE Data Extracts and/or Matched Datasets (as applicable). Any claims, liabilities and demands that have accrued under any previous agreements shall be dealt with under this Clause 30, unless the Parties agree otherwise in writing.

(iv) The Licence End Date may be extended at the discretion of DfE. Requests to extend the Licence End Date should be made in writing to the DfE Data Sharing Team using the email address data.sharing@education.gov.uk and an extension shall only be agreed when confirmed in writing by DfE.

(v) Unless terminated earlier in accordance with Clause 7, the Supplier's access to the Personal Data will terminate on the Licence End Date.

(vi) In accordance with the Mandatory Clauses, the Supplier must Destroy the Personal Data by the Licence End Date applicable to that Personal Data (or earlier if the Supplier no longer needs the

Personal Data in connection with the performance of its obligations as a Processor) and provide written evidence to DfE that demonstrates the data has been Destroyed.

(d) PROCESSING

(i) As stated in Clause 2, this section sets out the additional terms and conditions on which the Supplier will process Personal Data when providing services to DfE under the Agreement.

(ii) DfE and the Supplier acknowledge and agree that for the purpose of Data Protection Legislation DfE is the Controller and the Supplier is the Processor.

(iii) The Supplier shall at all times only process the Personal Data in accordance with the Mandatory Clauses and for the Permitted Use.

(iv) The Supplier shall provide DfE with the Permitted Intended Outputs in respect of the Supplier's processing of the Personal Data in accordance with the delivery dates set out in Special Terms Schedule 1, Table 2 unless agreed otherwise by the parties in writing.

(v) The transfer of the Personal Data between the parties under this Clause 30 shall be in accordance with the transfer method set out in Special Terms Schedule 1, Table 2.

(e) CONTACTS

(i) DfE shall specify its Data Protection Officer, primary contact and secondary contact in Special Terms Schedule 1, Table 1. DfE shall use reasonable endeavours to ensure that the same individuals perform those roles throughout the term of this Clause 30, but DfE may replace such individuals from time to time where reasonably necessary in the interests of DfE's activities.

(ii) The Supplier shall appoint a Data Protection Officer, primary contact and secondary contact, such persons as identified in Special Terms Schedule 1, Table 1. The Supplier shall use reasonable endeavours to ensure that the same individuals perform those roles throughout the term of this Clause 30, but the Supplier may replace such individuals from time to time where reasonably necessary in the interests of the Supplier's activities.

(f) TERMINATION

Except where specified to the contrary in this Clause 30 and without affecting any other right or remedy available to DfE, in the event that DfE wishes to terminate the provisions outlined in this Clause 30, DfE shall serve written notice to the named

primary and secondary contacts of the Supplier (as set out in Special Terms Schedule 1, Table 1). The termination date shall be determined by DfE based on what is deemed appropriate under the circumstances.

(g) CONFLICTS

If there is any conflict or inconsistency between any of the provisions of this Clause 30 and the provisions of the Agreement, the provisions of the Clause 30 shall prevail.

(h) VARIATION

No variation of this Clause 30 shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

Special Terms Schedule 1: DSAP requirements for the processing of the DfE Data Extracts and/or Matched Datasets (as applicable) by the Supplier

Data Sharing Approval Panel (DSAP) No:
DfE Reference No:
Name of Project:

Table 1 – Contact details of the parties :

DfE primary contact name, position, email address	data.sharing@education.gov.uk
DfE secondary contact name, position, email address	[redacted] [redacted]
DfE Data Protection Office name, telephone number, email address	DataProtection.OFFICE@education.gov.uk Department for Education, 7&8 Wellington Place, Wellington Street, Leeds, LS1 4AW

Supplier	BDO LLP
Supplier Primary Contact including name, position, telephone number, email address	[redacted] [redacted]
Supplier Secondary Contact including name, position, telephone number, email address	[redacted] [redacted]
Supplier Data Protection Officer name, address, telephone number, email address	[redacted] [redacted]
Commencement Date	The date of the Call-off signature
Licence End Date	Enter Licence End Date in format DD/MM/YY

Table 2 – Description of the DfE Data Extracts and/or Matched Datasets (as applicable) to be processed by the Supplier:

Personal Data (DfE Processed Data Extracts) to be provided to the Supplier	**SLC Data** • [redacted] • [redacted] It also covers the following non-Personal data: **HMRC Data** [redacted] • [redacted] • [redacted] • [redacted]
Personal Data provided to DfE for a Matching Request	N/A
Personal Data (Matched Dataset) to be provided to the Supplier	• Not Applicable
DfE classification of the Personal Data (DfE Data Extracts)	• The SLC data is Personal data with level 3 meaningless identifiers, Sensitivity level D • Some of it is special category personal data (data relating to health, disability and mortality).
DfE classification of the Personal Data (Matched Dataset)	Not applicable
Expected timescale for delivery of the Personal Data (DfE Data Extracts) to the Supplier for processing (from receipt of the signed call-off contract)	Initial delivery will be approximately 2-4 weeks after receipt of the signed call-off contract to get the new auditor up to speed with the methodology but after that the data will be delivered on an annual basis in April each year at the start of the audit process.
Expected timescale for delivery of the Personal Data (Matched Dataset) to	Not applicable

the Supplier for processing (from receipt of the signed call-off contract)	
Recipient of DfE data	[redacted] [redacted]
File format of the Personal Data (DfE Data Extracts) to be made available to the Supplier	**SLC Data** • [redacted]4GB • [redacted]3.9GB It also covers the following non-Personal data: **HMRC Data** • [redacted] • [redacted] • [redacted] • [redacted] • 637mb
File format of Personal Data (Matched Dataset) to be made available to the Supplier	N/A
Method of transfer	[redacted] (DfE preferred secure file transfer system)
Storage location of DfE data	[redacted]
Description of use of Personal Data permitted under this Agreement to be used in the details published on GOV.UK	Department for Education (DfE) wishes to share personal data (derived from HMRC and Student Loan Company data) relating to borrowers whose student loan repayments were sold in the 2017 and 2018 sale of Student Loans with those organisations who have a legal duty to assess the performance of the relevant Income Contingent Repayment (ICR) Student Loans. These organisations include: CSC Global (the issuer), investors via the Citibank website and auditors (Government Actuary Department, Ernst & Young, Price Waterhouse Cooper) and a valuation agency (Kroll). The rating agencies (S&P Global, Fitch) receive pseudonymised and aggregate data on request. The DfE Secretary of State, acting as “Master Servicer” of the Loans, must continue to annually notify each of the Sale 1

	and Sale 2 investors on the performance of the relevant Income Contingent Repayment (ICR) Student Loans, until such point as all the Loans are either repaid in full or are written off as per the conditions of the ICR Student Loan. Therefore the data share is required by law.
Permitted Use of the Personal Data (DfE Data Extracts)	The DfE Data Extracts shall be processed by the Supplier on behalf of DfE for academic research in respect of the following research project and to produce the Permitted Intended Outputs: • BDO will audit TERM (the Forecasting Model) as well as providing other audit services to ensure that TERM is functioning as expected and is seen to be the subject of external scrutiny (referred to as the Agreed Upon Procedure or AUP audit). BDO will independently recreates the Transition Matrices and other assumptions from the DfE Processed Data. They will not have access to the raw SLC data (as provided from SLC to DfE under the 2024 MoU), instead they will have access to the DfE Processed data created by DfE from the raw SLC data.
Permitted Use of the Personal Data (Matched Datasets)	Not applicable
Permitted Intended Outputs for the Personal Data (DfE Data Extracts)	The Supplier will be contracted to produce • Agreed Upon Procedure Audit Report (July each year) • Model Audit Report (July each year), one for each sale
Permitted Intended Outputs for the Personal Data (Matched Datasets)	Not applicable
Statistical Disclosure Control	The statistical disclosure control applied to permitted outputs from this project will be as outlined in the relevant sections (listed below) outlined within the “Statistical Disclosure Control (SDC) policy for DfE data”. The relevant sections of this policy document for this project are: A - General rules (for shares not including HESA or CiN / CLA):

Supplier Permitted User(s)	Only designated personnel of the Supplier are permitted to
Record keeping where Jisc data is shared (if required)	N/A
Special conditions (if any)	

Special Terms Schedule 2

Supplier Permitted Users

Annex 1 - Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

1.1.1.1 The contact details of the Relevant Authority's Data Protection Officer are [redacted]: (dataprotection.office@education.gov.uk)

1.1.1.2 The contact details of the Supplier's Data Protection Officer are: [redacted] or +44(0)207 893 3873

1.1.1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.1.1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	**The Relevant Authority is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: **SLC Data** [redacted] It also covers the following non-Personal data: **HMRC Data** • [redacted] **The Supplier is Controller and the Relevant Authority is Processor** *The Parties acknowledge that for the purposes of the Data* Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph 3 to paragraph 16 of the following Personal Data: • Not applicable

	The Parties are Joint Controllers The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of: • Not applicable **The Parties are Independent Controllers of Personal Data** *The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:* ● *Business contact details of Supplier Personnel for which the Supplier is the Controller,* ● *Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller,* Not applicable
Duration of the Processing	Data will be processed for the duration of the audit, for the contract year. Personal data will be returned or destroyed in line with the plan at the bottom on this table.
Nature and purposes of the Processing	Cleaning and processing data SLC and HMRC data, removing excluded borrowers as per pre-agreed exclusion reasons, allocating individuals into agreed earnings bands, aggregating data by earnings band and borrower age and gender. Performing smoothing and extrapolation calculations using information provided by DfE. Performing transformations of the data, checking the inputs of the stochastic model and checking the outputs are as expected. Purpose: statutory and regulatory obligations, to ensure a robust audit.
Type of Personal Data	Name, date of birth (Month and Year of Birth only), loan amount, region of study. Special category Personal data relating to Disability and Mortality.

Categories of Data Subject	Student loan borrowers and employees (HMRC data)
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	All data should either be returned to the Student Loan Company or destroyed. The auditor should store all personal data electronically where possible. However, all physical copies must be destroyed by the end of the contract year via shredding and incineration.

Annex 2 - Joint Controller Agreement – This Annex is not used for this agreement

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 3-16 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 18-28 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [Supplier/Relevant Authority]:

(i) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

(j) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(k) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;

(l) is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Deliverables where consent is the relevant legal basis for that Processing; and

(m) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier's/Relevant Authority's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. Undertakings of both Parties

1.1.2.1 The Supplier and the Relevant Authority each undertake that they shall:

(a) report to the other Party every [x] months on:

(i) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

(e) request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

(g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its

Personnel:

(i) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where that Party would not be permitted to do so; and

(iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and

(j) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.

1.1.2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

3. Data Protection Breach

1.1.3.1 Without prejudice to clause 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection

Legislation; and

(b) all reasonable assistance, including:

(i) cooperation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(ii) cooperation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(iii) coordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

1.1.3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

4. Audit

1.1.4.1 The Supplier shall permit:

(a) the Relevant Authority, or a third-party auditor acting under the Relevant

Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

(b) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Deliverables.

1.1.4.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

1.1.5.1 The Parties shall:

(a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

6. ICO Guidance

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. Liabilities for Data Protection Breach

1.1.7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

(a) if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents,

contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

(b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(c) if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree to such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).

1.1.7.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

1.1.7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

(a) if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.

1.1.7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment

of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Relevant Authority.

8. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 of the Core Terms (*Ending the contract*).

9. Sub-Processing

1.1.9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.