**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**

* 1. 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:
     1. “Controller” in respect of the other Party who is “Processor”;
     2. “Processor” in respect of the other Party who is “Controller”;
     3. “Joint Controller” with the other Party;
     4. “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**

* 1. 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.
  2. The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.
  3. 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:
     1. a systematic description of the envisaged Processing and the purpose of the Processing;
     2. an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
     3. an assessment of the risks to the rights and freedoms of Data Subjects; and
     4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
  4. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
     1. 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;
     2. 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:
        1. nature of the data to be protected;
        2. harm that might result from a Personal Data Breach;
        3. state of technological development; and
        4. cost of implementing any measures;
     3. ensure that :
        1. the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));
        2. 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:
           1. 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*);
           2. are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
           3. 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
           4. have undergone adequate training in the use, care, protection and handling of Personal Data;
     4. 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:
        1. 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;
        2. the Data Subject has enforceable rights and effective legal remedies;
        3. 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
        4. 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
     5. 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.
  5. Subject to paragraph 7 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:
     1. receives a Data Subject Access Request (or purported Data Subject Access Request);
     2. receives a request to rectify, block or erase any Personal Data;
     3. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
     4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
     5. 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
     6. becomes aware of a Personal Data Breach.
  6. The Processor’s obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
  7. 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 6 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
     1. the Controller with full details and copies of the complaint, communication or request;
     2. 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;
     3. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
     4. assistance as requested by the Controller following any Personal Data Breach; and/or
     5. 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.
  8. 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:
     1. the Controller determines that the Processing is not occasional;
     2. 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
     3. the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
  9. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller’s designated auditor.
  10. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
  11. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
      1. notify the Controller in writing of the intended Subprocessor and Processing;
      2. obtain the written consent of the Controller;
      3. 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
      4. provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
  12. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
  13. 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).
  14. 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**

* 1. 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**

* 1. 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.
  2. 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.
  3. Where a Party has provided Personal Data to the other Party in accordance with paragraph 8 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.
  4. 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.
  5. The Parties shall only provide Personal Data to each other:
     1. to the extent necessary to perform their respective obligations under the Contract;
     2. 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
     3. where it has recorded it in Annex 1 *(Processing Personal Data).*
  6. 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.
  7. 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.
  8. 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”)**:
     1. 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
     2. 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:
        1. 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
        2. 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.
  9. 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:
     1. do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
     2. implement any measures necessary to restore the security of any compromised Personal Data;
     3. 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
     4. 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.
  10. 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).*
  11. 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)*.
  12. 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 27 of this Joint Schedule 11.

## 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. The contact details of the Relevant Authority’s Data Protection Officer are: [dp.enquiries@service.education.gov.uk](mailto:dp.enquiries@service.education.gov.uk)

Please copy the authority’s contract manager, as outlined within the order form.

* + - 1. The contact details of the Supplier’s Data Protection Officer are: **<redacted>**
      2. The Processor shall comply with any further written instructions with respect to Processing by the Controller.
      3. 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 2 to paragraph 15 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:   * This contract does not explicitly require, nor have as a core purpose, the processing of personal data; however, personal data may be processed if respondents have included personal information in error, when completing their form. |
| Duration of the Processing | For the duration of the contract and for any possible extensions. |
| Nature and purposes of the Processing | The nature of the Processing means any operation such as recording, organisation, structuring, storage, retrieval, consultation, use, restriction, erasure or destruction of data (whether or not by automated means) etc.  The purpose might include: statutory obligation and assessment of questionnaire results and/or development of insight reports (e.g the final report). |
| Type of Personal Data | Names of organisations, potentially names of schools/workplaces. quantitative data (ie response type: eg parent/teacher etc) and long-form qualitative responses to a number of policy-based questions |
| Categories of Data Subject | Customers/ clients, members of the public; e.g. all people who completed a questionnaire submission. |
| 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 | The data will be retained for the duration of the contract period and its extensions, all data will be destroyed by deletion (for digital media) or incineration (for any physical media) once the contract is concluded. |

**Annex 2 - Joint Controller Agreement**

* + 1. **Undertakings of both Parties**
       1. The Supplier and the Relevant Authority each undertake that they shall:
    2. report to the other Party **every 3 months** on:
       1. the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);
       2. the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
       3. 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;
       4. any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
       5. 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;

* + 1. notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
    2. 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;
    3. 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;
    4. request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;
    5. 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;
    6. 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:
       1. are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;
       2. 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 the that Party would not be permitted to do so; and
       3. have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;
    7. ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:
       1. nature of the data to be protected;
       2. harm that might result from a Personal Data Breach;
       3. state of technological development; and
       4. cost of implementing any measures;
    8. 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
    9. ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.
       1. 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.
    10. **Data Protection Breach**
        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:
    11. 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
    12. all reasonable assistance, including:
        1. co-operation 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;
        2. co-operation 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;
        3. co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or
        4. 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.
        5. 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:
    13. the nature of the Personal Data Breach;
    14. the nature of Personal Data affected;
    15. the categories and number of Data Subjects concerned;
    16. the name and contact details of the Supplier’s Data Protection Officer or other relevant contact from whom more information may be obtained;
    17. measures taken or proposed to be taken to address the Personal Data Breach; and
    18. describe the likely consequences of the Personal Data Breach.
    19. **Audit**
        1. The Supplier shall permit:
    20. 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
    21. 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. 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.
    22. **Impact Assessments**
        1. The Parties shall:
    23. 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
    24. 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.
    25. **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.

* + 1. **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*).

* + 1. **Sub-Processing**
       1. In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:
    2. 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
    3. ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.
    4. **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.