

DATA PROCESSOR AGREEMENT

CONTENTS

CLAUSE

1.	Definitions and interpretation	2
2.	Personal data types and processing purposes	3
3.	Supplier's obligations	4
4.	Supplier's personnel	5
5.	Security	6
6.	Personal Data Breach.....	6
7.	Cross-border transfers of personal data	8
8.	Subcontractors	9
9.	Complaints, data subject requests and third party rights	9
10.	Term and termination	10
11.	Data return and destruction	11
12.	Records	11
13.	Audit.....	12
14.	Warranties	13
15.	Indemnification	14
16.	Freedom of Information Act 2000 / Environmental Information Regulations 2004.....	14
17.	Notice.....	15

ANNEXES

ANNEX A	Personal Data Processing Purposes and Details	17
ANNEX B	Security Measures	22

BACKGROUND

- (A) The School and the Supplier entered into **Service Level and Licence Agreement** that may require the Supplier to process Personal Data on behalf of the School
- (B) This DPA contains the mandatory clauses required by Article 28(3) of the retained EU Law version of the General Data Protection Regulations ((EU) 2016/679) (UK GDPR) for contracts between controllers and processors.
- (C) Personal Data Processing Agreement (**DPA**) sets out the additional terms, requirements and conditions on which the Supplier will process Personal Data when providing services under the Service Level and Licence Agreement

AGREED TERMS

Terms defined in the DPA

Expressions defined in the DPA and used herein shall have the meaning set out in the DPA.

Governing law

This DPA and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of England and Scotland.

Jurisdiction

Each party irrevocably agrees that the courts of England and Scotland shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this deed or its subject matter or formation (including non-contractual disputes or claims).

1. Definitions and interpretation

The following definitions and rules of interpretation apply in this DPA.

1.1 Definitions:

Authorised Persons: the persons or categories of persons that the School authorises to give the Supplier personal data processing instructions as identified in ANNEX A and from whom the Supplier shall solely accept such instructions.

Business Purposes: the services described in the Service Level and Licence Agreement or any other purpose specifically identified in ANNEX A.

Controller: as defined by the Data Protection Act 2018, Section 3(6)

Data Protection Legislation: all applicable privacy and data protection laws including without limitation the General Data Protection Regulations 2016 ((EU) 2016/679) as retained in UK law (UK GDPR), the Data Protection Act 2018 and any applicable laws, regulations and secondary legislation in England and Scotland

relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426).

Data Subject: as defined by the Data Protection Act 2018, Section 3(5)

Personal Data: as defined by the Data Protection Act 2018, Section 3(2)

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Processing and process: as defined by the Data Protection Act 2018, Section 3(4)

Processor: as defined by the Data Protection Act 2018, Section 3(6)

Standard Contractual Clauses (SCC): the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU and as may be amended or updated from time to time.

This DPA is subject to the terms of the Service Level and Licence Agreement and is incorporated into the Service Level and Licence Agreement. Interpretations and defined terms set forth in the Service Level and Licence Agreement apply to the interpretation of this DPA.

1.2 The Annexes form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Annexes.

1.3 In the case of conflict or ambiguity between:

- (a) any provision contained in the body of this DPA and any provision contained in the Annexes, the provision in the body of this DPA will prevail;
- (b) the terms of any accompanying invoice or other documents annexed to this DPA and any provision contained in the Annexes, the provision contained in the Annexes will prevail; and
- (c) any of the provisions of this DPA and the provisions of the Service Level and Licence Agreement, the provisions of this DPA will prevail

2. Personal data types and processing purposes

2.1 The School and the Supplier acknowledge that for the purpose of Data Protection Legislation, the School is the controller and the Supplier is a processor.

- 2.2 The School retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Supplier.
- (a) ANNEX A describes the subject matter, duration, nature and purpose of processing and the Personal Data categories and Data Subject types in respect of which the Supplier may process to fulfil the Business Purposes of the Service Level and Licence Agreement.
 - (b) The parties recognise that the school may, as detailed in Annex A, send data categorised under Article 9 of the GDPR. The parties understand that the school will do so under the lawful basis of Article 9(2)(g) public interest

3. Supplier's obligations

- 3.1 The Supplier will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the School's written instructions from Authorised Persons. The Supplier will not process the Personal Data for any other purpose or in a way that does not comply with this DPA or Data Protection Legislation. The Supplier must promptly notify the School if, in its opinion, the School's instruction would not comply with Data Protection Legislation.
- 3.2 The Supplier will comply at all times with the requirements of Data Protection Legislation and guidance from the Information Commissioner and other relevant regulator and perform its obligations under this DPA in such a way as to ensure that the School does not or is not likely to breach any of its obligations under Data Protection Legislation.
- 3.3 The Supplier must promptly comply with any School request or instruction from Authorised Persons requiring the Supplier to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.
- 3.4 The Supplier will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the School or this DPA specifically authorises the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires the Supplier to process or disclose Personal Data, the Supplier must first inform the School of the legal or regulatory requirement and give the School an opportunity to object or challenge the requirement, unless the law prohibits such notice or where it would not be reasonably practicable to do so.
- 3.5 The Supplier will reasonably assist the School, at no additional cost to the School, with meeting the School's compliance obligations under Data Protection Legislation in respect of this DPA and the Service Level and Licence Agreement, taking into account the nature of the Supplier's processing and the information available to the Supplier, including in relation to Data Subject

rights, data protection impact assessments and reporting to, cooperating and consulting with supervisory authorities under Data Protection Legislation.

- 3.6 The Supplier must notify the School within two (2) Working Days if it receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this DPA, where it may legally do so.
- 3.7 The Supplier must provide reasonable assistance to the School in responding to any such communication within the timescales set out by the regulatory authority, and within reasonable timescales requested by the School during any consultation with the regulatory authority for the purpose of checking compliance of data processing with the Act.
- 3.8 The Supplier must promptly notify the School of any changes to Data Protection Legislation that may adversely affect the Supplier's performance of the Service Level and Licence Agreement.
- 3.9 The Supplier must employ a data protection officer if required by law.
- 3.10 The Supplier will only collect Personal Data for the School using a notice or method that the School specifically pre-approves in writing, which contains an approved data privacy notice informing the Data Subject of the School's identity and its appointed data protection representative, the purpose or purposes for which their Personal Data will be processed, and any other information that, having regard to the specific circumstances of the collection and expected processing, is required to enable fair processing. The Supplier will not modify or alter the notice in any way without the School's prior written consent.
- 3.11 Both parties are reminded that nothing within this DPA relieves the parties of their own direct responsibilities and liabilities under Data Protection Legislation. Each party may be subject to investigative and corrective powers of supervisory authorities (such as the ICO); if they fail to meet their obligations, they may be subject to an administrative fine or penalty and they may have to pay compensation.

4. Supplier's personnel

- 4.1 The Supplier will ensure that all personnel (including employees, volunteers, consultants, etc):
 - (a) are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;
 - (b) have undertaken training on Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties, which is repeated on a regular basis; and

- (c) are aware both of the Supplier's duties and their personal duties and obligations under Data Protection Legislation and this DPA.

4.2 The Supplier will take reasonable steps to ensure the reliability, integrity and trustworthiness of, and conduct background checks consistent with applicable law on, all of the Supplier's personnel with access to the Personal Data.

5. Security

5.1 The Supplier must at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in B. The Supplier must document those measures in writing and review them annually to ensure they remain current and complete.

5.2 The Supplier must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

- (a) the pseudonymisation and encryption of personal data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- (d) a procedure for regularly testing, assessing and evaluating the effectiveness of security measures.

6. Personal Data Breach

6.1 The Supplier will promptly and without undue delay notify the School if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable ("compromised"). Where such Personal Data has been compromised due to the Supplier acts or omissions, the Supplier will restore such Personal Data at its own expense.

6.2 The Supplier will immediately and without undue delay notify the School if it becomes aware of:

- (a) any accidental, unauthorised or unlawful processing of the Personal Data; or
- (b) any Personal Data Breach.

- 6.3 Where the Supplier becomes aware of (a) and/or (b) above, it shall, without undue delay, also provide the School with the following information:
- (a) description of the nature of (a) and/or (b), including the categories and approximate number of both Data Subjects and Personal Data records concerned;
 - (b) the likely consequences; and
 - (c) description of the measures taken or proposed to be taken to address (a) and/or (b), including measures to mitigate its possible adverse effects.
- 6.4 Immediately following any unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. The Supplier will reasonably co-operate with the School in the School's handling of the matter, including:
- (a) assisting with any investigation;
 - (b) providing the School with physical access to any facilities and operations affected;
 - (c) facilitating or undertaking interviews with the Supplier's employees, former employees and others involved in the matter, and sharing results with the School as appropriate;
 - (d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the School; and
 - (e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Personal Data processing.
- 6.5 Neither Party shall inform any third party of any Personal Data Breach without first obtaining the other's prior written consent, except when required to do so by law. We recognise that notification of data subjects, DPOs, the ICO, and discussion under confidence with experts, are examples of requirement by law
- 6.6 The Supplier agrees that the School has the sole right to determine:
- (a) whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in the School's discretion, including the contents and delivery method of the notice; and
 - (b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.
- 6.7 The Supplier will cover all reasonable expenses associated with the performance of the obligations under clause 6.2 and clause 6.4 unless the matter arose from the School's specific instructions, negligence, wilful default or breach of this DPA in which case the School will cover all reasonable expenses.

6.8 The Supplier will also reimburse the School for actual reasonable expenses that the School incurs when responding to a Personal Data Breach to the extent that the Supplier caused such a Personal Data Breach, including all costs of notice and any remedy as set out in clause 6.6. To the extent permitted in law, the Supplier's liability under this clause 6.8 shall be limited to the sums paid by the School to the Supplier in the 12 months preceding the Personal Data Breach.

7. Cross-border transfers of personal data

7.1 The Supplier (or any subcontractor) must not transfer or otherwise process Personal Data outside the UK without obtaining the School's prior written consent.

7.2 Where such consent is granted, the Supplier may only process, or permit the processing, of Personal Data outside the UK under one of the following conditions:

- (a) UK Adequacy Regulations
the Supplier is processing Personal Data in a country, territory, sector or international organisation which is covered by UK 'adequacy regulations'. The Supplier must identify in ANNEX A the country, territory, sector or organisation that is subject to such an adequacy finding and the Supplier must immediately inform the School of any change to that status; or
- (b) Appropriate Safeguards
the Supplier participates in a valid cross-border transfer mechanism under Data Protection Legislation, so that the Supplier (and, where appropriate, the School) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the General Data Protection Regulations (*UK GDPR*). The Supplier must identify in ANNEX A the transfer mechanism that enables the parties to comply with these cross-border data transfer provisions and the Supplier must immediately inform the School of any change to that status; or
- (c) Exceptions to Article 46
the transfer otherwise complies with Data Protection Legislation on the basis of an exception as set out in Article 46 of the General Data Protection Regulations (*UK GDPR*). The Supplier must identify in ANNEX A the exception that enables the parties with these cross-border data transfer provisions and the Supplier must immediately inform the School of any change to that status.

7.3 If any Personal Data transfer between the School and the Supplier requires execution of SCC in order to comply with Data Protection Legislation (where the School is the entity exporting Personal Data to the Supplier), the parties will complete all relevant details in, and execute, the SCC, and take all other actions required to legitimise the transfer.

8. Subcontractors

8.1 The Supplier may only authorise a third party (subcontractor) to process the Personal Data if:

- (a) the School provides prior written consent prior to the appointment of each subcontractor;
- (b) the Supplier enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this DPA, in particular, in relation to requiring appropriate technical and organisational data security measures, facility for audit when required; and, upon the School's written request, provides the School with copies of such contracts;
- (c) the Supplier maintains control over all Personal Data it entrusts to the subcontractor; and
- (d) the Supplier ensures that the subcontractor's sub-processing contract in respect of this DPA terminates automatically on termination of this DPA for any reason, for the avoidance of doubt, the Supplier shall not be required to cease all contractual agreements with its subcontractor in respect of other supply contract that the Supplier has in place.

8.2 Those subcontractors approved as at the commencement of this DPA are as set out in ANNEX A. The Supplier must list all approved subcontractors in Annex A and include any subcontractor's name and location and contact information for the person responsible for privacy and data protection compliance.

8.3 Where the subcontractor fails to fulfil its obligations under such written agreement, the Supplier remains fully liable to the School for the subcontractor's performance of its agreement obligations.

8.4 The Parties consider the Supplier to be responsible for any Personal Data in the possession of its subcontractors as supplied by the Supplier to the subcontractor pursuant to the Service Level and Licence Agreement or this DPA..

8.5 On the School's reasonable written request, the Supplier will audit a subcontractor's compliance with its obligations regarding the School's Personal Data and provide the School with the audit results.

9. Complaints, data subject requests and third party rights

9.1 The Supplier must, at no additional cost, take such technical and organisational measures as may be appropriate, and promptly provide such information to the School as the School may reasonably require, to enable the School to comply with:

- (a) the rights of Data Subjects under Data Protection Legislation, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and
- (b) information or assessment notices served on the School by any supervisory authority under Data Protection Legislation.

9.2 The Supplier must notify the School immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with Data Protection Legislation pursuant to this DPA or the Service Level and Licence Agreement.

9.3 The Supplier must notify the School within 2 working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under Data Protection Legislation.

9.4 The Supplier, at no additional cost to the School, will give the School its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 The Supplier must not disclose the Personal Data to any Data Subject or to a third party other than at the School's request or instruction, as provided for in this DPA or as required by law.

9.6 The Supplier shall, following notification from the School that it has received a request from a third party seeking information under FOI, send to the School within (2) Working Days the information requested by the School and, in addition, any additional information that it holds on behalf of the School under this DPA that the Supplier believes (acting reasonably) is relevant to the FOI request

9.7 The Supplier shall not respond to any request for information (including Personal Data) received by it under FOI that it holds on behalf of the School without consultation with the School.

10. Term and termination

10.1 This DPA will remain in full force and effect so long as:

- (a) the Service Level and Licence Agreement remains in effect, or
- (b) the Supplier retains any Personal Data related to the Service Level and Licence Agreement in its possession or control (**Term**).

- 10.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Service Level and Licence Agreement in order to protect Personal Data will remain in full force and effect.
- 10.3 The Supplier must appoint (in writing) a representative within the UK if required by law.
- 10.4 The Supplier's failure to comply with the terms of this DPA is a material breach of the Service Level and Licence Agreement. In such event, the School may terminate the Service Level and Licence Agreement effective immediately on written notice to the Supplier without further liability or obligation.
- 10.5 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Service Level and Licence Agreement obligations, the parties will suspend the processing of Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with Data Protection Legislation within one calendar month, they may terminate the Service Level and Licence Agreement on written notice to the other party.

11. Data return and destruction

- 11.1 At the School's request, the Supplier will give the School a copy of or access to all or part of the School's Personal Data in its possession or control in the format and on the media reasonably agreed between the parties..
- 11.2 On termination of the Service Level and Licence Agreement for any reason or expiry of its term, the Supplier will securely delete or destroy or, if directed in writing by the School, return and not retain, all or any Personal Data related to this DPA in its possession or control.
- 11.3 If any law, regulation, or government or regulatory body requires the Supplier to retain any documents or materials that the Supplier would otherwise be required to return or destroy, it will notify the School in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.
- 11.4 The Supplier will certify in writing that it has destroyed the Personal Data within 5 working days after it completes the destruction.

12. Records

- 12.1 The Supplier will keep detailed, accurate and up-to-date written records regarding any processing of Personal Data it carries out for the School, including but not limited to, the

access, control and security of the Personal Data, approved subcontractors and affiliates, the processing purposes, categories of processing, any transfers of personal data to a country outside of the UK and related safeguards, and a general description of the technical and organisational security measures referred to in clause 5.1.

12.2 The Supplier will ensure that the Records are sufficient to enable the School to verify the Supplier's compliance with its obligations under this DPA and the Supplier will provide the School with copies of the Records upon request.

12.3 The School and the Supplier must review the information listed in the Annexes to this DPA once a year to confirm its current accuracy and update it when required to reflect current practices.

13. Audit

13.1 No more than once every 12 months and upon giving no less than two week's advance notice to the Supplier, the Supplier will permit the School and its third-party representatives to audit the Supplier's compliance with its DPA obligations during the Term. The Supplier will audit its agreed sub-contractors on the same terms when required. The Supplier will give the School and its third-party representatives all necessary reasonable assistance to conduct such audits. The assistance may include, but is not limited to:

- (a) physical access to, remote electronic access to, and copies of the Records and any other information held at the Supplier's premises or on systems storing Personal Data that is the subject of this DPA;
- (b) access to and meetings with any of the Supplier's personnel reasonably necessary to provide all explanations and perform the audit effectively; and
- (c) inspection of all Records and the infrastructure, electronic data or systems, facilities, equipment or application software used to store, process or transport Personal Data that is the subject of this DPA.

13.2 The notice requirements in clause 13.1 will not apply if the School reasonably believes that a Personal Data Breach occurred or is occurring, or the Supplier is in breach of any of its obligations under this DPA or any Data Protection Legislation.

13.3 If a Personal Data Breach occurs or is occurring, or the Supplier becomes aware of a breach of any of its obligations under this DPA or any Data Protection Legislation, the Supplier will:

- (a) promptly conduct its own audit to determine the cause;
- (b) produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;
- (c) provide the School with a copy of the written audit report; and

- (d) remedy any deficiencies in respect of its data processing obligations under this DPA as identified by the audit within 5 working days.

13.4 At least once a year, the Supplier will conduct site audits of its Personal Data processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this DPA, The Supplier will produce a written report that includes detailed plans to remedy any security deficiencies identified by the audit.

13.5 On the School's written request, the Supplier will make all of the relevant audit reports available to the School for review. The School will treat such audit reports as the Supplier's confidential information under this DPA, subject to requirements of law, for example the Freedom of Information Act 2000 or Environmental Information Regulations 2004.

13.6 The Supplier will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by the Supplier's management.

14. Warranties

14.1 The Supplier warrants and represents that:

- (a) its employees, agents and any other person or persons accessing Personal Data on its behalf have received the required training on Data Protection Legislation relating to the Personal Data;
- (b) it and anyone operating on its behalf will process the Personal Data in compliance with Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;
- (c) it has no reason to believe that Data Protection Legislation prevents it from providing any of the Service Level and Licence Agreement's contracted services; and
- (d) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:
 - (i) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage;
 - (ii) the nature of the Personal Data protected; and
 - (iii) comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in clause 5.1.

14.2 The School warrants and represents that the Supplier's expected use of the Personal Data for the Business Purposes and as specifically instructed by the School will comply with Data Protection Legislation.

14.3 The Supplier shall hold and ensure that it continues to hold throughout the term of this DPA a satisfactory level of and appropriate insurance cover with a reputable insurer to cover the Data Processor's obligations to the School under this DPA, including without limitation, public liability cover of at least five million pounds sterling. The Data Processor will disclose to the School satisfactory evidence of such insurance (including the amount and type of cover effected) and payment of current premiums as soon as reasonably practicable upon request by the School.

15. Indemnification

15.1 The Supplier agrees to indemnify, keep indemnified and defend at its own expense the School against all costs, claims, damages or expenses incurred by the School or for which the School may become liable due to any failure by the Supplier or its employees, subcontractors or agents to comply with any of its obligations under this DPA or Data Protection Legislation.

15.2 The Supplier's liability under this DPA shall be limited to £500,000.

15.3 The Supplier shall have no liability to the School, whether arising in contract, tort (including negligence), breach of statutory duty or otherwise, for or in connection with loss, interception or corruption of any data resulting from any negligence or default by any provider of data transfer services;

16. Freedom of Information Act 2000 / Environmental Information Regulations 2004

16.1 The Supplier acknowledges that the School is subject to the requirements of the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) and shall assist and co-operate with the School to enable the School to comply with these requirements.

16.2 The Supplier shall and shall procure that its Sub-contractors shall:

- (a) transfer all Requests for Information to the School as soon as practicable after receipt and in any event within two (2) working days of receiving a Request for Information;
- (b) provide the School with a copy of all Information in its possession or power in the form that the School requires within five (5) working days (or such other period as the School may specify) of the School requesting that Information; and

- (c) provide all necessary assistance as reasonably requested by the School to enable the School to respond to a Request for Information within the time for compliance set out in section 10 of the FOIA or Regulation 5(2) of the EIR.

- 16.3 The School shall be responsible for determining in its absolute discretion whether the Commercially Sensitive Information and/or Confidential Information and/or any other Information:
 - (a) is exempt from disclosure under the FOIA and the EIR; and
 - (b) is to be disclosed in response to a Request for information.

- 16.4 In no event shall the Supplier respond directly to a Request for Information unless expressly authorised to do so by the School.

- 16.5 The Supplier acknowledges that the School may, acting in accordance with the Department of Constitutional Affairs' Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of FOIA ("the Code") be obliged under the FOIA, or the EIR to disclose information concerning the Supplier or the Services:
 - (a) in certain circumstances without consulting with or obtaining consent from the Supplier; or
 - (b) following consultation with the Supplier and having taken its views into account.

- 16.6 Provided always that where 16.5(a) applies the School shall, in accordance with any recommendations of the Code, take reasonable steps, where appropriate, to give the Supplier advanced notice, or failing that, to draw the disclosure to the Supplier's attention after any such disclosure.

- 16.7 The Supplier shall ensure all information submitted in connection with the tendering process or in the course of the DPA or relating to the DPA is retained for disclosure and shall permit the School to inspect such records as requested from time to time.

- 16.8 The Supplier acknowledges that any lists or schedules provided by it as part of the tendering process outlining the Supplier's Confidential Information and Supplier's Commercially Sensitive Information are of indicative value only and that the School may nevertheless be obliged to disclose Confidential Information in accordance with this Clause.

17. Notice

- 17.1 Any notice or other communication given to a party under or in connection with this DPA must be in writing and delivered to:


(a) For the School: (e.g. Headteacher) responsible for Service Level and Licence Agreement

(b) For the Supplier: sally.bliwert@assessment360.org

17.2 clause 17.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

17.3 A notice given under this DPA will be valid if sent by email to the email addresses as agreed in writing between the parties and if accompanied by a delivery receipt.

17.4 This DPA has been entered into on the date stated at the beginning of it.

For and on behalf of:		For and on behalf of:	
(the Data Controller)		[The Supplier] (the Data Processor)	
Authorised Signatory name:		Authorised Signatory name:	Sally Bliwert
Signature:		Signature:	
Date		Date	

ANNEX A Personal Data Processing Purposes and Details

1 **Subject matter of processing:**

Turas360 is an assessment system that allows schools to track progress through the Curriculum for Excellence and analyse pupil attainment alongside attendance, attitude to learning, and wellbeing data.

2 **Duration of Processing:**

The Supplier will process the Personal Data for the duration of the agreement.

3 **Nature of Processing:**

The data is being supplied to allow a pupil's academic achievements to be recorded in Turas360 alongside other relevant information that the school may use to analyse and improve pupil attainment.

4 **Business Purposes:**

An online system that will allow schools to assess and plan against the Curriculum for Excellence using either the Supplier exemplar framework or their own custom framework to track the progress of pupils through the curriculum. The system will support pupil input and personal next steps so that each child can engage with their own learning and enable school staff to analyse the data at individual, class, year, and group level using contextual groups such as FSM, EAL, etc. Attendance can be populated automatically from the school MIS (if Xporter is being used), which can be combined with recording Attitude to Learning and pupil Wellbeing for a complete picture of each child.

5 **Personal Data Categories:**

The Personal Data transferred or to be transferred concerns the following categories of Data Subjects (please tick or mark as N/A as appropriate):

Advisers, consultants and other experts	n/a
Agents and contractors	n/a
Business or other contacts	n/a
Complainants, correspondents and enquirers	n/a
Donors and lenders	n/a
Landlords or tenants	n/a
Members, alumni or supporters	n/a
Offenders and suspected offenders	n/a

Service Users/Schools/clients/patients	✓
Previous and prospective employers of the staff and referees	n/a
Relatives, guardians, and associates of the data subject	n/a
Staff including volunteers, agents, temporary and casual workers	✓
Pupils/students	✓
Suppliers	n/a
Others – please specify below	n/a

6 **Data Subject Types:**

Please tick or mark as N/A as appropriate

Identifying information – names and former names, dates of birth, reference numbers (e.g. UPN, employee number), etc.	✓
Contact information – postal and email addresses (current and former), telephone number	✓
Education/training records and examination results	✓
Employment details	✓
Family lifestyle and social circumstances	n/a
Financial details	n/a
Goods and/or services provided	n/a
<i>Special Categories of Personal Data as defined by the Act:</i>	
Criminal allegations, proceedings, outcomes and sentences	n/a
Physical or mental health or condition	✓
Politics	n/a
Racial or ethnic origin	n/a
Religion or other beliefs of a similar nature	n/a
Sex life	n/a
Sexual orientation	n/a
Trade union membership	n/a
Genetics	n/a
Biometrics (where used for ID purposes)	n/a
<i>Others – please specify below</i>	

Attendance data	✓
Wellbeing and attitude to learning information	✓

7 Privacy Notices

The below information should be added to the 'Details of any external data processors' section of the Full Privacy Notice in order to comply with the transparency principle.



Turas360 (curriculum assessment)

Student data processed: name, data of birth, UPN, gender, email address, attendance data, ALN data, pupil assessments, attitude to learning and wellbeing rankings. Images, notes, audio files, and videos of pupil work completed and pupils for evidence.

Staff data processed: name, employee number, work email address, IP address, browser information, device information, user actions on Turas360 system.

Turas360 is used to track pupil progress through the curriculum and can be linked with the school MIS using a data extractor (Xporter) that extracts information. Data is stored on Amazon Web Services (AWS) servers by Assessment360 (London) and Xporter (Europe). Data at rest is protected behind the Virtual Private Cloud (VPC) and is encrypted when at rest using industry standard AES-256 encryption. Xporter syncs data every 2-4 hours for those schools that opt for automation and third-party apps choose to import data overnight daily.

<https://assessment360.org/privacy-policy/>

8 Return and destruction of data

The Supplier will process the Personal Data for the duration of the Service Contract. The Supplier will do the following on termination of the Service Level and Licence Agreement for any reason or expiry of its term:

- 8.1 retain Personal Data in line with Section 11 of this DPA and will securely delete or destroy or (if directed in writing by the School) return Personal Data belonging to the School in its possession or control within a maximum period of 8 weeks or such other time as the parties agree in writing.
- 8.2 certify in writing that Supplier has destroyed the Personal Data within 5 working days after it completes the destruction.

9 **Approved Subcontractors:**

Subcontractor Name	Reason for using subcontractor	Privacy Information
Amazon Web Services (UK registration - 08650665)	Electronic data storage, cloud server and transmission service.	AWS GDPR DPA.pdf (awsstatic.com) GDPR - Amazon Web Services (AWS)
Blueberry Consultants Ltd (03293060)	Backup technical support.	https://www.bbconsult.co.uk/aboutus/privacypolicy
Xero (UK registration - 06071722)	Invoicing. Xero contains Headteacher names and email addresses	Xero and GDPR: Protecting your personal data Xero UK Data Processing Terms Xero UK

10 **Additional information**

The Supplier has added some additional features, including:

10.1 Multi-Pupil Assess

The ability to assess multiple pupils at once. Schools will be able to make assessment against several or even all pupils within that class at once by selecting a class or group. This allows teachers to see (at a glance) the stage of all pupils for each E and O.

10.2 Customise Assessment Frameworks and the Exemplar Framework

With flexibility in mind, the Supplier has built into Turas360 the ability for schools to customise their own assessment frameworks within the system.

For its initial release, Turas360 will be available with a choice of two frameworks:

- 10.2.1 the Es and Os as laid out in the Curriculum for Excellence document and a customised sample framework - the Exemplar Framework.
- 10.2.2 Schools are able to design and upload their own customised assessment frameworks by creating their own sub-statements.

11 **Plan Across Multiple Areas**

Plans can be constructed using statements from all six Areas alongside statements from the Literacy and Numeracy Framework (LNF) and Digital Competence Framework (DCF) allowing you to track everything in one place - including planning for the Four Purposes.

12 **General**

- 12.1 The Data Processor shall comply with any further written instructions with respect to processing by the School.
- 12.2 Any such further instructions shall be incorporated into this Annex, or communicated in writing to the Data Processor.

ANNEX B Security Measures

All data is stored on Amazon Web Servers based in London, UK. Pupil data is stored, backed up, processed and managed within the UK by the Supplier staff.

1. Physical access controls.

SCHOOL: conducts vetting checks on their staff (i.e. DBS) who are subject to data protection and online safety policies/procedures, acceptable user agreements, and contractual confidentiality clauses. All staff receive data protection, cyber security, and safeguarding training on an annual basis.

COMPANY: The Supplier staff with access to the data receive mandatory data awareness training. The Cloud Systems Manager (CSM) is responsible for configuring and maintaining the servers and has his work reviewed regularly. The Supplier monitors work logs for all staff. Software developers work using demo data.

2. System access controls.

SCHOOL: control staff access to information by ensuring staff have the appropriate system access for their roles. For example:

Job Role	Access Type & Purpose
Headteacher & Senior Management Team	To review whole school, class, and individual pupil pages. The role requires full access for tracking pupil progress, editing data when needed (i.e. wellbeing/attitudes to learning), and reporting statistics on class and/or whole school progress.
Teaching Staff	To review whole class and selected individual pupil pages. The role requires view/edit access to data so it can be maintained and utilised for assessment purposes (i.e. to track pupil progress alongside the needs of the Curriculum for Excellence framework).
Applicable administration staff (i.e. School Clerk or equivalent)	To manually upload data from SIMS database (where applicable). Administration staff otherwise have no need to view or edit school/, class, and individual pupil pages. Access to data should be restricted to comply with data protection Principle (c) of the UK GDPR.

The school network is maintained and monitored by the Local Authority via an SLA to ensure security measures are in place (i.e. web filtering, etc.).

COMPANY: The Supplier have four classes of staff within the organisation. These are Managerial (ad hoc access to data); Support and Technical (daily responsibility for data); and Financial (billing purposes). All support staff members are located in the UK and trained in responsible handling of data. All laptops are encrypted, and all customer

data stored in SharePoint Online is encrypted (with one or more AES 256-bit keys). Access to the database and servers are restricted to only essential staff members using MFA.

3. Data access controls.

COMPANY: Data access requires authentication using work email address. All pupil data is stored on Amazon Web Services (AWS) servers based in London, UK. Pupil data is stored, backed up, processed, and managed within the UK by the Supplier staff. System user (i.e. staff) data is stored in several locations. All are held in EU and UK based data centres:

In the system servers, AWS. Data is encrypted at rest using industry standard AES-256 encryption on UK servers. Information is accessed by staff with adequate training and permissions.

In the events booking system, Microsoft Forms. Data is encrypted at rest in EU servers.

In the cloud storage, Microsoft365. Data is encrypted at rest in EU servers and accessed by staff with relevant job function and training in data protection.

Username, title, and email address will be transferred directly from the school MIS (i.e. SIMS) to Turas360 using the Xporter API link. Alternatively, data can be supplied manually by encrypted file transfer at the point the system is set up for a school or updated.

4. Transmission controls.

Data will be manually transferred by encrypted file transfer at the point the system is set up for a school or updated. Schools are requested to send data updates when they occur. This is done using a secure file transfer site provided by the Supplier.

5. Input controls.

COMPANY: Auditing is built into Turas360 and the Supplier support team will be responsible for maintaining the audit logs. All updates to the database are logged beforehand with the SQL used, the person requesting, and the staff member executing the SQL.

6. Data backups.

COMPANY: The Supplier maintains daily backups of the last 35 days. The backups are encrypted and held in AWS data centres located in the UK. Data at rest is protected behind the Virtual Private Cloud (VPC) and is encrypted when at rest using industry standard AES-256 encryption.