Data Processing Agreement

This Agreement is entered into on the Effective Date.

Parties

(1) The customer accepting this DPA electronically **(Customer)**

(2) **EQUIN LIMITED** incorporated and registered in England and Wales with company number 06347232 whose registered office is at Unit G Pattern Shop, Trevoarn, Hayle, Cornwall, TR27 4EZ **(Supplier)**

Background

(A) The Customer and the Supplier entered into Terms of Service **(Master Agreement)** that may require the Supplier to process Personal Data on behalf of the Customer.

(B) This Personal Data Processing Agreement **(Agreement)** sets out the additional terms, requirements and conditions on which the Supplier will process Personal Data when providing services under the Master Agreement. This Agreement contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*) for contracts between controllers and processors.

Agreed Terms

1. Definitions and Interpretation

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

1.1. Definitions

Authorised Persons	the persons or categories of persons that the Customer authorises to give the Supplier written personal data processing instructions as identified in Annex A and from whom the Supplier agrees solely to accept such instructions.
Business Purposes	the services to be provided by the Supplier to the Customer as described in the Master Agreement and any other purpose specifically identified in Annex A.
Commissioner	the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).
Controller	has the meaning given in section 6, DPA 2018.
Data Protection Legislation	all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (**DPA 2018**); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the Commissioner or other relevant regulatory authority and which are applicable to a party.
Data Subject	the identified or identifiable living individual to whom the Personal Data relates.
EEA	the European Economic Area.
EU GDPR	the General Data Protection Regulation ((EU) 2016/679).

Personal Data	means any information relating to an identified or identifiable living individual that is processed by the Supplier on behalf of the Customer as a result of, or in connection with, the provision of the services under the Master Agreement.
Personal Data Breach	a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data.
Processing, processes, processed, process	any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third-parties.
Processor	a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.
Records	has the meaning given in Clause 12.
Term	this Agreement's term as defined in Clause 10.
UK GDPR	has the meaning given in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

1.2. This Agreement is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this Agreement.

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

1.4. A reference to writing or written excludes fax but not email.

1.5. In the case of conflict or ambiguity between:

(a) any provision contained in the body of this Agreement and any provision contained in the Annexes, the provision in the body of this Agreement will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in the Annexes, the provision contained in the Annexes will prevail; and

(c) any of the provisions of this Agreement and the provisions of the Master Agreement, the provisions of this Agreement will prevail.

2. Personal data types and processing purposes

2.1. The Customer and the Supplier agree and acknowledge that for the purpose of the Data Protection Legislation:

(a) the Customer is the Controller and the Supplier is the Processor.

(b) the Customer retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to,

providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the Supplier.

(c) Annex A describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which the Supplier may process the Personal Data to fulfil the Business Purposes.

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 Customer'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 Agreement or the Data Protection Legislation. The Supplier must promptly notify the Customer if, in its opinion, the Customer's instructions do not comply with the Data Protection Legislation.

3.2. The Supplier must comply promptly with any Customer written instructions requiring the Supplier to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3. The Supplier will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third-parties unless the Customer or this Agreement specifically authorises the disclosure, or as required by domestic law, court or regulator (including the Commissioner). If a domestic law, court or regulator (including the Commissioner) requires the Supplier to process or disclose the Personal Data to a third-party, the Supplier must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the domestic law prohibits the giving of such notice.

3.4. The Supplier will reasonably assist the Customer, at no additional cost to the Customer, with meeting the Customer's compliance obligations under the Data Protection Legislation, 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 and consulting with the Commissioner or other relevant regulator under the Data Protection Legislation.

3.5. The Supplier must notify the Customer promptly of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting the Supplier's performance of the Master Agreement or this Agreement.

3.6. The Customer acknowledges that it is responsible for ensuring that any Personal Data uploaded to the Supplier's system has been collected in accordance with applicable data protection laws, including providing appropriate privacy notices to Data Subjects. The Customer warrants that it has obtained all necessary consents or has other applicable legal bases for the processing of Personal Data by the Supplier in accordance with this Agreement.

4. Supplier's employees

4.1. The Supplier will ensure that all of its employees:

(a) are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data;

(b) have undertaken training on the Data Protection Legislation and how it relates to their handling of the Personal Data and how it applies to their particular duties; and

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

5. Security

5.1. The Supplier must at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the 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 the following link https://www.insighttracking.com/security

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 process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6. Personal data breach

6.1. The Supplier will without undue delay notify the Customer in writing if it becomes aware of:

(a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data. The Supplier will restore such Personal Data at its own expense as soon as possible.

(b) any accidental, unauthorised or unlawful processing of the Personal Data; or

(c) any Personal Data Breach.

6.2. Where the Supplier becomes aware of (a), (b) and/or (c) above, it will, without undue delay, also provide the Customer with the following written information:

(a) description of the nature of (a), (b) and/or (c), including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

(b) the likely consequences; and

(c) a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.

6.3. Immediately following any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, the Supplier will reasonably co-operate with the Customer at no additional cost to the Customer, in the Customer's handling of the matter, including but not limited to:

(a) assisting with any investigation;

(b) providing the Customer with physical access to any facilities and operations affected;

(c) facilitating interviews with the Supplier's employees, former employees and others involved in the matter including, but not limited to, its officers and directors;

(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 Customer; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data processing.

6.4. The Supplier will not inform any third-party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the Customer's written consent, except when required to do so by domestic law.

6.5. The Supplier agrees that the Customer has the sole right to determine:

(a) whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Customer'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.

6.6. The Supplier will cover all reasonable expenses associated with the performance of the obligations under clause 6.1 to clause 6.3 unless the matter arose from the Customer's specific written instructions, negligence, wilful default or breach of this Agreement, in which case the Customer will cover all reasonable expenses.

7. Transfers of personal data

7.1. The Supplier (and any sub-processor) must not transfer or otherwise process the Personal Data outside the area consisting of the UK and EEA without either ensuring that an appropriate safeguard is in place (as required under the UK GDPR) or, if not, obtaining the Customer's prior written consent.

8. Sub-processors

8.1. The Supplier may only authorise a third-party (sub-processor) to process the Personal Data if:

(a) the Customer is provided with an opportunity to object to the appointment of each sub-processor within 30 working days after the Supplier supplies the Customer with full details in writing regarding such sub-processor;

(b) the Supplier enters into a written contract with the sub-processor that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Customer's written request, provides the Customer with copies of the relevant excerpts from such contracts;

(c) the Supplier maintains control over all of the Personal Data it entrusts to the sub-processor.

8.2. Those sub-processors approved as at the commencement of this Agreement are as set out in Annex A. The Supplier must list all approved sub-processors in Annex A and include any sub-processor's name and location.

8.3. Where the sub-processor fails to fulfil its obligations under the written agreement with the Supplier which contains terms substantially the same as those set out in this Agreement, the Supplier remains fully liable to the Customer for the sub-processor's performance of its agreement obligations.

8.4. The Parties agree that the Supplier will be deemed by them to control legally any Personal Data controlled practically by or in the possession of its sub-processors.

9. Complaints, data subject requests and third-party rights

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

(a) the rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the rights to rectify, port 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 Customer by the Commissioner or other relevant regulator under the Data Protection Legislation.

9.2. The Supplier must notify the Customer immediately in writing 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 the Data Protection Legislation.

9.3. The Supplier must notify the Customer within 7 days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

9.4. The Supplier will give the Customer, at no additional cost to the Customer, 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 in accordance with the Customer's written instructions, or as required by domestic law.

10. Term and termination

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

(a) the Master Agreement remains in effect; or

(b) the Supplier retains any of the Personal Data related to the Master Agreement in its possession or control **(Term)**.

10.2. Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect the Personal Data will remain in full force and effect.

10.3. The Supplier's failure to comply with the terms of this Agreement is a material breach of the Master Agreement. In such event, the Customer may terminate any part of the Master Agreement involving the processing of the Personal Data effective immediately on written notice to the Supplier without further liability or obligation of the Customer.

10.4. If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Master Agreement obligations, the parties may agree to suspend the processing of the Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within 30 days, either party may terminate the Master Agreement with immediate effect on written notice to the other party.

11. Data return and destruction

11.1. At the Customer's request, the Supplier will give the Customer, or a third-party nominated in writing by the Customer, a copy of or access to all or part of the Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

11.2. On termination of the Master Agreement for any reason or expiry of its term, the Supplier will securely delete or destroy or, if directed in writing by the Customer, return and not retain, all or any of the Personal Data related to this Agreement in its possession or control.

11.3. If any law, regulation, or government or regulatory body requires the Supplier to retain any documents, materials or Personal Data that the Supplier would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the

documents, materials or Personal Data that it must retain, the legal basis for such retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

12. Records

12.1. The Supplier will keep detailed, accurate and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, approved sub-processors, the processing purposes, categories of processing, and a general description of the technical and organisational security measures referred to in Clause 5.1 **(Records)**.

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

12.3. The Customer and the Supplier must review the information listed in the Annexes to this Agreement annually to confirm its current accuracy and update it when required to reflect current practices.

13. Audit

13.1. The Supplier will permit the Customer and its third-party representatives to audit the Supplier's compliance with its Agreement obligations, once per calendar year, with an additional audit permitted in the event of a suspected data breach, upon thirty [30] days' prior written notice (or seven [7] days' notice for breach-related audits), provided that all auditors execute appropriate confidentiality agreements and maintain strict confidentiality regarding all information accessed during the audit. Whilst the Supplier will not provide usernames, passwords, or direct platform access credentials, the Supplier will provide all necessary data and assistance to conduct such audits at no additional cost to the Customer. 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 the Personal Data;

(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 process the Personal Data.

13.2. The notice requirements in Clause 13.1 will not apply if the Customer reasonably believes that a Personal Data Breach has occurred or is occurring, or the Supplier is in material breach of any of its obligations under this Agreement or any of the 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 Agreement or any of the Data Protection Legislation, the Supplier will notify the Customer as soon as reasonably practicable and carry out an audit to investigate the breach.

14. Warranties

14.1. The Supplier warrants and represents that:

(a) its employees, agents and any other person or persons accessing the Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation;

(b) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

(c) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Master 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 accidental, unauthorised or unlawful processing of Personal Data and the loss or damage to, the Personal Data, and ensure a level of security appropriate to:

(i) the harm that might result from such accidental, unauthorised or unlawful processing and loss 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 Customer warrants and represents that the Supplier's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

15. Indemnification

15.1. The Supplier agrees, subject to any limitations on liability in the Master Agreement to indemnify, at its own expense the Customer against costs or damages incurred by the Customer or for which the Customer may become liable due to any failure by the Supplier or its employees, sub-processors or agents to comply with any of its obligations under this Agreement and/or the Data Protection Legislation.

15.2. Any limitation of liability set forth in the Master Agreement will apply to this Agreement's indemnity or reimbursement obligations.

16. Notice

16.1. Any notice given to a party under or in connection with this Agreement shall be in writing and shall be:

(e) delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case); or

(f) sent by email to the following addresses (or an address substituted in writing by the party to be served):

(i) For the Customer: such email address as may have been provided to the Supplier by the Customer or otherwise in use by the Customer

(ii) For the Supplier: dpo@equin.co.uk

16.2. Any notice shall be deemed to have been received:

(a) if delivered by hand, at the time the notice is left at the proper address;

(b) if sent by pre-paid first-class post or other next working day delivery service, at 9:00am on the second Business Day after posting

(c) if sent by email, at the time of transmission, or, if this time falls outside Business Hours in the place of receipt, when Business Hours resume.

16.3. This clause 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.

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

Annex A Personal Data processing purposes and details

Subject matter of processing
The Supplier supplies cloud-based software to educational institutions on an annual subscription basis. The software is used to track pupil assessments, monitor academic progress, and support development. It enables schools and educational bodies to manage detailed pupil data and generate customisable reports to analyse and improve educational outcomes.

Duration of Processing
For the duration of the Services provided under this agreement.

Nature and Purpose of Processing

- **Pupil records:** Includes identifiers (e.g. UPN), legal/preferred names, date of birth, gender, enrolment status, and optional attributes such as ethnicity, EAL status, FSM history, SEN history, service child status, in-care status, attendance summaries, custom groups, notes, photos, and contacts. Used to manage pupil information and support tailored reporting and analysis.
- **Assessment data:** Includes statutory and internal assessments, test scores, teacher judgements, and supporting evidence (e.g. images, written comments, and attachments).
- **User profiles**: Collection of names, email addresses, passwords, roles, and access levels for Customer employees and Authorised Users to enable access and support.
- **System logs**: Automated logs for diagnostic and performance monitoring purposes. May contain limited personal data (e.g. UPNs, pupil assessments, user email address). Retained for 45 days.
- **Email support:** Customers may share personal data via support emails, including pupil or user information. Retained for up to 36 months. Deletion available on request.
- **Call recordings**: Calls to Customer Support may be recorded for training and monitoring. Retained for 12 months. Deletion available on request.

Business Purposes
To enable Customers to track pupil data, assess performance, and generate reports using various pupil attributes for analysis and improvement of educational outcomes.

Categories of Personal Data

- **Pupil records**: UPN, names, DOB, gender, enrolment dates.
- **Optional pupil data**: Address, ethnicity, EAL, FSM, SEN, service child/in-care status, attendance, groups, notes, photo, contacts.
- **Assessment data**: EYFSP, Phonics, SATs, test results, teacher judgements, supporting evidence.
- **User data**: Name, email, access level, role, password.
- **Support data**: Data shared via support emails, call recordings, system logs.

Categories of Data Subjects

- Pupils
- Customer employees
- Authorised users

Sub-processor List

Entity	Purpose	Location
Amazon Web Services, Inc.	Hosting infrastructure used to store, process and transmit Customer Data.	United Kingdom
RavenDB Ltd.	Cloud-based database hosting used to store Customer Data.	United Kingdom
Wonde Limited	Processing and importing Customer Data into the Services.	United Kingdom
Aircall SAS	Provision of telephony services in support of Customer support activities.	Germany
FrontApp, Inc.	Email management services used for Customer support activities.	Ireland
Microsoft Limited	Tools used to assist with Customer support activities.	United Kingdom
Slack Technologies Limited	Internal communication platform used to assist with Customer support.	United Kingdom