



Applicaa Data Processing Agreement

1 Definitions

1.1 In this Data Processing Agreement, unless the context otherwise requires, the following words and expressions have the following meanings:

"Agreement"	the agreement for the supply of services entered into by the parties consisting of this Data Processing Agreement in conjunction with the Contractor's standard Terms and Conditions
"Commencement Date"	means the date of this Agreement
"Confidential information"	means all confidential information (however recorded or preserved) disclosed by The School to Applicaa Ltd in connection with this Agreement, which is either labelled as such or else which could be reasonably considered confidential because of its nature and the manner of its disclosure
"Contractor Personnel"	means all directors, officers, employees, agents, consultants and contractors of the Contractor and/or any Sub-contractor or Sub-processor engaged in the performance of its obligations under this Agreement
"Data Controller"	has the meaning given in the Data Protection Act 2018 as amended or replaced from time-to-time
"Data Loss Event"	any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement
"Data Processor"	has the meaning given in the Data Protection Act 2018 as amended or replaced from time-to-time
"Data Protection Officer"	has the meaning given in the Data Protection Act 2018 as amended or replaced from time-to-time

“Data Protection Legislation”	means the General Data Protection Regulation (EU 2016/679) (GDPR), the Data Protection Act 2018, and national implementing laws, regulations and secondary legislation, as amended or updated from time to time in the UK, and all applicable law about the processing of Personal Data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner. This includes post-Brexit legislation in the UK such as the UK General Data Protection Regulation (2021).
“Data Subject”	has the meaning given in the Data Protection Act 2018 as amended or replaced from time-to-time
“GDPR”	refers to both the General Data Protection Regulation (EU 2016/679), and the UK General Data Protection Regulation (2021).
“Personal Data”	has the meaning given in the Data Protection Act 2018 as amended or replaced from time-to-time and relates only to Personal Data, or any part of such Personal Data, of which the Customer is the Data Controller and in relation to which the Contractor is providing services under the Agreement
“Processing”	has the meaning given in the Data Protection Act 2018 as amended or replaced from time-to-time
“Personal Data Breach”	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.
“Sub-processor”	means any third Party appointed to process Personal Data on behalf of the Contractor related to this Agreement

1.2

For the purposes of this Data Processing Agreement, School is referred to as “Customer” and Applica Ltd will be referred to as the “Contractor”, together the “parties”.

1.3

In the event of any inconsistency between this Data Processing Agreement and the data protection provisions (including clause 8) of the Contractor’s standard Terms and Conditions governing the supply of the Contractor’s services, this Data Processing Agreement shall prevail. The Contractor’s standard Terms and Conditions shall govern the other aspects of the relationship between the Contractor and the Customer, including payment terms, termination and liability provisions and provisions on access to the Services.

2. Basis for Processing or Sharing

2.1

Both parties will comply with all applicable requirements of the Data Protection Legislation. This Data Processing Agreement is in addition to and does not relieve, remove or replace the parties' obligations under the Data Protection Legislation.

2.2

The parties acknowledge that for the purposes of this Agreement, the Customer is the Data Controller and the Contractor is the Data Processor of any Personal Data.

2.3

The basis for processing and sharing Personal Data under this Agreement is in accordance with a lawful basis for processing Personal Data provided for by the Data Protection Legislation. The details of the data processing activities in relation to this Agreement are set out in Annex A.

3. Obligations of the Contractor

3.1

The Contractor shall only process any Personal Data on behalf of the Customer in accordance with the written instructions provided and to the extent, and in such manner as set out in Annex A. If the Contractor is required to do otherwise by law then it will promptly notify the Customer of the legal requirement before processing the Personal Data.

3.2

The Contractor shall provide reasonable assistance to the Customer in preparation of any data protection impact assessment required prior to the commencement of any processing.

3.3

The Contractor will maintain complete and accurate records of any processing of Personal Data it carries out on behalf of the Customer.

3.4

If the Contractor receives any complaint, notice or communication which relates directly or indirectly to the processing or sharing of Personal Data or to either party's compliance with the Data Protection Legislation, it shall promptly notify the Customer and provide full cooperation and assistance in relation to any such complaint, notice or communication.

3.5

Taking into account the nature of the Personal Data to be protected, the harm that might arise from an event described in this clause, the state of technological development and the cost of implementing any measures, the Contractor shall ensure that it has in place appropriate technical and organisational measures in relation to the processing of Personal Data by the Contractor, to protect against unauthorised or unlawful processing of the Personal Data and against the accidental or unlawful destruction, loss, alteration,

unauthorised disclosure of, or access to the Personal Data and to protect against a Data Loss Event arising as a result of any acts or omissions by the Contractor.

In particular, the Contractor shall reasonably endeavour to ensure a level of security appropriate to the risk, including as appropriate:

3.5.1 The pseudonymisation and encryption of the Personal Data;

3.5.2 The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

3.5.3 The ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident;

A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

3.6

The Contractor shall immediately inform the Customer if any Personal Data is lost or destroyed or becomes damaged, corrupted or unusable. The Contractor will restore such Personal Data at its own expense.

3.7

The Contractor shall notify the Customer immediately if it becomes aware of any (a) accidental, unauthorised or unlawful processing of Personal Data or (b) any Personal Data Breach and in either case shall comply with all reasonable requests of the Customer in dealing with the situation.

3.7.1 Where the Contractor becomes aware of any matters in (a) or (b) above, it shall also provide the Customer with the following information:

3.7.1.1 A description of the nature of the matters set out in (a) and/or (b) above, including the categories and approximate number of both Data Subjects and Personal Data records concerned;

3.7.1.2 The likely consequences; and

3.7.1.3 A description of the measures taken, or proposed to be taken, to address the matters set out in (a) and/or (b) above, including measures to mitigate its possible adverse effects.

3.8

The Contractor shall cooperate with the Customer and take such reasonable steps as directed by the Customer to assist in the investigation, mitigation and remediation of each Data Loss Event or Personal Data Breach.

3.9

Upon termination of the Agreement for any reason or upon request by the Customer, the Contractor shall cease processing of any Personal Data and shall return all Personal Data to the Customer and any copies thereof, or shall securely destroy all Personal Data if instructed

to do so by the Customer - and shall certify that this has been done (unless prevented from doing so by law) within 30 days of the request being made, with possible reasonable extension of this timeframe up to 60 days or more as otherwise agreed between the parties.

This shall not apply to data stored as part of the company-wide backup of the entire cloud database, which is held in an encrypted format and not normally accessible to Applica staff. This backup is held for two years, and is necessary in case of a catastrophic data centre failure, and individual student records cannot be deleted from this backup. Because this backup is 'beyond the reach' of Applica staff, this has been ruled to conform to UK GDPR standards by the ICO's office (see this URL for further details:

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/storage-limitation/>

3.10

The Customer may in its absolute discretion by written notice from the Data Protection Officer to the Contractor at any time require the Contractor to return a complete copy of all Customer data in the media reasonably specified by the Customer and at a reasonable cost to the Customer.

3.11

The Customer may in its absolute discretion by written notice at any time from the Data Protection Officer require the Contractor to delete and use all reasonable endeavours to procure the deletion of all other copies of the Customer's data processed by the Contractor or any of its sub-processors. The Customer acknowledges that exercise of its rights under this clause does not constitute termination of the Agreement unless it follows the termination procedures set out in the Contractor's standard Terms and Conditions and that the Contractor shall be entitled to continue making charges for the services as set out in the Agreement until the Agreement is validly terminated.

3.12

The Contractor and its Sub-processors may retain Customer data to the extent required by any applicable law, provided that the Contractor and its Sub-contractors shall ensure the confidentiality of all such data retained and shall ensure that such data is only processed as necessary for the purposes specified by applicable laws requiring its storage and for no other purpose. The Customer acknowledges that the Contractor may use anonymised usage information to monitor use of the Services and that the Contractor may access the Customer Data for the purposes of providing support and maintenance, and to audit the Customer's use of the Services under the Contract.

4 Transfers outside EEA

4.1

The Contractor shall not transfer any Personal Data outside of the UK or the European Economic Area (EEA) unless the following conditions are fulfilled:

4.1.1 the Contractor ensures that there are appropriate safeguards in place in relation to the transfer pursuant to Article 45 of the GDPR;

4.1.2 the Contractor ensures that the transfer is to a country approved by the European Commission as providing adequate protection for Personal Data pursuant to Article 45 of the GDPR or one of the derogations for specific situations in Article 49 of the GDPR applies to the transfer;

4.1.3 the Data Subject has enforceable rights and effective legal remedies;

4.1.4 the Contractor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection for any Personal Data that is transferred; and

4.1.5 the Contractor complies with reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data.

4.1.6 the contractor first informs the data controller of the intention to move data outside of the EEA. A DPIA will be required in the first instance.

5. Contractor's Personnel

5.1

The Contractor shall ensure that access to the Personal Data is limited to those Personnel who need access to the Personal Data to meet the Contractor's obligations under this Agreement.

5.2

The Contractor shall ensure that all Personnel:

5.2.1 are aware of both the Contractor's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement;

5.2.2 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 Customer or as otherwise permitted by this Agreement

5.2.3 are subject to appropriate confidentiality undertakings with the Contractor or any Sub-processor

5.2.4 have undertaken adequate training on the Data Protection Legislation relating to the use, care, protection and handling of Personal Data

6. Rights of Data Subject

6.1

The Contractor shall notify the Customer immediately if it or one of its Sub-processors:

6.1.1 receives a request from a Data Subject for access to that person's Personal Data

6.1.2 receives a request to rectify, block or erase any Personal Data

6.1.3 receives a request from any third party for disclosure of Personal Data where compliance with such a request is required or purported to be required by Law; or

6.1.4 becomes aware of a Data Loss Event

6.2

The Contractor shall provide the Customer with full co-operation and assistance in relation to any request referred to in clause 6.1

6.3

The Contractor shall promptly comply with any request from the Customer requiring the Contractor to amend, transfer or delete the Personal Data where such operations are unable to be performed by the Customer. The Contractor is entitled to provide a reasonable charge to the Customer.

6.4

The Contractor shall not disclose the Personal Data to any Data Subject or to a third party other than at the request of the Customer or as provided by this Data Processing Agreement.

6.5 The Contractor shall designate a Data Protection Officer if required by Data Protection Legislation.

7. Rights of the Customer

7.1

The Contractor will make available all information necessary to the Customer to demonstrate compliance with UK GDPR obligations - and allow for the Customer to contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the controller. Such audits to be carried out in accordance with the provisions of clause 7.2

7.2

The Customer is entitled, on giving reasonable notice to the Contractor to inspect or appoint representatives to inspect all facilities, equipment, documents and electronic data relating to the processing of Personal Data by the Contractor within standard business hours. The Customer shall ensure that it or any nominated auditor avoid (or if it cannot avoid, minimise) any damage, injury or disruption to the Contractor's or its Sub-processors' premises, equipment, personnel and business.

7.3

If following an inspection, the Customer reasonably believes that any Personnel of the Contractor are causing the Contractor to be in breach of the Data Protection Legislation then the Customer may request that the Contractor no longer uses such Personnel for the purposes of handling Personal Data under this Agreement.

7.4

The Customer has the right to make reasonable objections to any changes or appointments of Sub-processor by the Contractor.

8. Warranties

8.1

Subject to the Customer's responsibilities under clauses 2.3 and 3.5, the Contractor warrants that:

8.1.1 it will process and share the Personal Data in compliance with the Data Protection Legislation and all other applicable laws, enactments, regulations, orders standards and other similar instruments

8.1.2 it will take such appropriate technical and organisational measures in order to ensure the safety and security of the Personal Data as may be specified from time to time by the Customer; and

8.1.3 it will take appropriate technical and organisational measures against the unauthorised and unlawful processing of Personal Data and against the accidental loss or destruction of, or damage to, Personal Data

9. Indemnity

9.1

The Contractor agrees to indemnify the Customer and keep indemnified and defend at its own expense against all costs, claims, damages or expenses incurred by the Customer or for which the Customer may become liable due to any failure by the Contractor or its Personnel to comply with the Data Protection Legislation or any of its other obligations under this Data Processing Agreement (including its schedules).

9.2

The Contractor shall take out insurance to cover any payment that may be required under clause 9.1

10. Appointment of Sub-processors

10.1

The Contractor shall not sub-contract any activity that will involve the processing of Personal Data to a Sub-processor without the Customer's prior written authorisation. The Contractor shall not engage (nor permit any Sub-Processor to engage) any third party (including any Processor) (or any replacement) for carrying out any processing of Personal Data without the Customer's prior written authorisation. As at the Commencement Date, the Customer has authorised use of those Sub-processors listed in Annex C and the appointment of replacement Sub-processors appointed by the Contractor in accordance with Clause 10.2.

10.2

Without prejudice to Clause 10.1 Contractor may only authorise a Sub-processor to process Personal Data if:

10.2.1 the Contractor supplies to the Customer with full details of any and all Sub-processors, whether engaged or proposed;

10.2.2 the Customer is provided with an opportunity to object to the appointment within 5 business days after the Contractor supplies the Customer with full details of the Sub-processors engaged and proposed;

10.2.3 the Contractor enters into a written agreement with the Sub-processor that gives effect to the terms set out in this Agreement such that they apply to the Sub-processor; and

10.2.4 the Sub-processor does not continue to process the Customer's Personal Data on termination of the Agreement for any reason.

10.3

The Contractor shall remain fully liable for all acts or omissions of any Sub-processor.

10.4

Without prejudice to Clause 10.2 the Contractor shall consider all reasonable objections made by the Customer in the choice of Sub-processor to be used; the remedy for an unresolved objection is termination of the affected service, not a sub-processor veto.

11. Liability

11.1 The liability provisions of the Contractor's standard terms and conditions shall apply to all liability arising under this Data Processing Agreement. In addition, the Contractor shall have no liability to the Customer whether arising in contract, tort (including negligence), breach of statutory duty, or otherwise, for or in connection with:

11.1.1 loss, interception or corruption of any data; other than to the extent that such loss is caused by the negligence or breach of the Contractor or one of its appointed Sub-processors

11.1.2 loss, interception or corruption of any data resulting from any negligence or default by any provider of telecommunications services to the Contractor or the Customer

12. Review

12.1

Any amendments to this Data Processing Agreement will become effective when agreed in writing between the parties and it may be reviewed to ensure continued compliance with Data Protection Legislation and guidance issued by the Information Commissioner's Office.

13. Third parties

No person who is not a party of this Agreement shall have any rights under this Agreement, whether pursuant to the Contracts (Rights of Third Parties) Act 1999 or otherwise.

14. Governing law

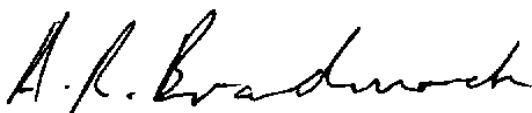
This Agreement and any dispute or claim made arising out of or in connection with it or its subject matter or formation shall be governed by the laws of England and Wales. The parties irrevocably agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement.

15. AI-assisted processing

Where the Processor provides AI-assisted features, the Processor shall:

- (a) process Controller Personal Data only as needed to respond to the user's request or carry out the task they have asked for;
- (b) act only on the Controller's documented instructions, including where a user chooses to use the assistant to work with special category data (for example, equality-monitoring analysis);
- (c) ensure the AI sub-processor is bound by obligations consistent with Article 28 UK GDPR;
- (d) ensure Controller Personal Data is not used to train AI models and is not retained by the AI provider beyond what is needed to return the response;
- (e) process such data within the EU/EEA; and
- (f) not use the assistant to make solely-automated decisions producing legal or similarly significant effects about an individual (UK GDPR Article 22).

Signed: For and on behalf of Applica Ltd:



Name: Andrew Bradnock
Position: DPO
Date: 11th June 2026 (effective 15th June 2026)

Signed: For and on behalf of:

Name:
Position:
Date:

Annex 1

Processing, Personal Data and Data Subjects

Description	Details
Subject matter of the processing	<i>Student data including: Admissions & Student Bursary Data</i>
Duration of the processing	<i>Data is deleted as soon as the contract is terminated.</i>
Nature and purpose of the processing	<i>To help the Schools process applications more efficiently; including the AI Assistant.</i>
Lawful basis of the processing	(Applicable to state schools:) Public task: <i>the processing is necessary for Schools to perform the task of admitting students for education in the public interest/for official functions, and for administering student bursaries.</i> (Applicable to independent schools:) Fulfilment of a contract
Type of Personal Data	<i>Student personal details and any data requested by the school, which may include special category data such as medical/health, SEND, ethnicity etc. family financial data., etc.</i>
Categories of Data Subject	<i>The admissions form is fully customisable so the school can collect any data it would like. Applicaa does not take any responsibility for the questions asked to parents; and information collected by the school.</i>
Plan for return and destruction of the data once the processing is complete.	<i>Schools can export data whenever they need to. As soon as the subscription is terminated or expires the data shall be removed and destroyed.</i>
Data storage location	<i>Amazon WES</i>
Point of contact for sharing this data - Name: - Position: - Contact email address: - Contact phone number: - Address:	<i>Antony Wambua COO antony@applicaa.com 020 4 538 1630 Wyevale Business Park King's Acre Hereford Herefordshire HR4 7BS</i>

Annex 2

Security Measures adopted by the Processor

Please insert details of your technical and organisational security measures, such as:

Item	Provider response
Physical access controls	No physical access to the data. All the servers are on cloud computer which is secured by Amazon Web Services.
System access controls	Servers (web servers, database servers) can only be accessed by the lead technical member, IP address is restricted in the UK, using encrypted connection.
Data access controls	Only school Staff members can access/manage student data in their school. Each staff member has different permissions to access different student data sections.
Transmission controls	No data will be transferred outside of the EU.
Input controls	Student details can only be input by Student, Parent and Teacher using registered accounts at Applica.
Data backups	Amazon RDS and Amazon S3 backups.
Data segregation	Servers are located in different availability zones (each zone is in different regions, at least 3 in London) so that if one server has a problem, the service is not disrupted.
Personnel checks, training,	Applica staff are trained regularly on data security (including GDPR), data processing, security procedure.
Other controls	

Annex 3

Please see below for a list of our sub-processors and the nature of their processing. All of the sub-processors have their GDPR compliance annually checked by Applicaa.

Sub-processor	Used for:	Location	Notes
Amazon Web Services	Storage of main Applicaa Databases	UK	
AccessPay	BACS bureau / Direct Debit mandate processing	UK	
Anthropic (via AWS Bedrock)	AI assistant (“Emma”) — generating responses and carrying out requested tasks	European Union	Data processing terms in place; data remains in the EU/EEA (covered by UK adequacy — no additional international-transfer mechanism required); not retained by the provider; not used for training
Esendex	SMS messaging services	UK	
Google Workspace (G-Suite)	Internal email system	UK	
Hubspot	Customer Database and Technical Support ticket logging.	USA	This Data Transfer with the USA is safeguarded by relevant Standard Contractual Clauses.
Postcode Look-Ups	Address lookup services	UK	
SendGrid/Twilio	SMTP Mail forwarding	USA	This Data Transfer with the USA is safeguarded by relevant Standard Contractual Clauses.
Slack	Internal messaging and collaboration	USA	This Data Transfer with the USA is safeguarded by

			relevant Standard Contractual Clauses.
Sub-processor	Used for:	Location	Notes
Stripe	Payment processing	USA	This Data Transfer with the USA is safeguarded by relevant Standard Contractual Clauses.
Xero	Accounting System	USA	This Data Transfer with the USA is safeguarded by relevant Standard Contractual Clauses.
Zoom	Video conferencing	USA	This Data Transfer with the USA is safeguarded by relevant Standard Contractual Clauses.

Additionally, some contractor staff within our business operate outside of the EEA, however all staff are subject to the same company Security and Acceptable Usage policies, and data processed by these teams are protected by UK GDPR-compliant International Data Transfer Agreements.

Change History:

v1.1 (revised 12 may 2022):

- Updated document to reflect name of post-Brexit UK GDPR legislation (2021).
- Corrected typographical error in paragraph 3.12 replacing 'X' with 'Contractor'
- Added 'fulfilment of contractor' as grounds for processing for independent schools.

v1.2 (revised 8 August 2022):

- Added reference to student/family financial data to cover the new Bursary+ product.

v2.0 (revised 19 October 2022):

- Amended name of the agreement to "Data Sharing Agreement"
- Added reference to processing by overseas staff and protection of this processing by UK GDPR-compliant International Data Transfer Agreements.

V2.1 (revised 28 October 2022):

- Amended name of the agreement to “Data Processing Agreement”

V2.2 (revised 4 July 2023):

- Added language referring to data being retained in the secure unencrypted backup, in line with ICO guidance.

V2.5 (revised 11 June 2026; effective 15 June 2026):

- Updated signature section.

- Updated for Emma AI