Applicaa Data Processing Agreement

Between the School and Applicaa Ltd, and, upon accession, the School's Local Authority

Parties

This Agreement is made between:

1. **Applicaa Ltd**, Wyevale Business Park, King's Acre, Hereford, Herefordshire, HR4 7BS ("the Processor" / "Applicaa");
2. **The School** identified in the Acceptance Record ("the School" / "Controller A"); and
3. **The Local Authority** in whose area the School is situated, as recorded in the Department for Education's Get Information About Schools register ("the LA" / "Controller B"). The LA becomes a party to this Agreement only from the date it accepts it in accordance with clause 16 (the "LA Activation Date"); until that date the LA has no rights or obligations under this Agreement.

The School and the LA are together "the Controllers"; all parties bound at the relevant time are together "the parties". This Agreement is accepted electronically by each party (clause 16); no wet signature is required.

1 Definitions

In this 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 Agreement in conjunction with the Processor's standard Terms and Conditions.

"Agreed Purposes" the purposes for which the Controllers share and process the Shared Personal Data, namely: post-16 destination tracking; identification of and support for young people who are or are at risk of becoming NEET; September Guarantee and statutory participation duties; and attendance monitoring in support of those purposes.

"Commencement Date" for each party, the date on which that party accepts this Agreement in accordance with clause 16.

"Controller" has the meaning given in the Data Protection Legislation. Each of the School and the LA is a separate, independent Controller of the Personal Data whose purposes and means it determines.

“Data Loss Event” any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement.

“Data Protection Legislation” the UK GDPR, the Data Protection Act 2018, and all national implementing laws and secondary legislation, as amended, and all applicable law and ICO guidance about the processing of Personal Data and privacy, including the ICO Data Sharing Code of Practice and the Age Appropriate Design Code (Children's Code).

“LA Activation Date” the date on which the LA accepts this Agreement in accordance with clause 16.

“Local Authority / LA” the local authority in whose area the School is situated, as recorded from time to time in the Department for Education's Get Information About Schools (GIAS) register, exercising its statutory functions in relation to young people's education, training, participation and attendance. If the School's recorded local authority changes, the register governs.

“Permitted Recipients” the parties, and the personnel of each Controller who need access to the Shared Personal Data for the Agreed Purposes.

“Personal Data Breach” a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

“Shared Personal Data” the Personal Data shared under Part B, as described in Annex 4. It flows one way, from the School to the LA, and may include attendance data and Special Category Data.

“Special Category Data” Personal Data revealing the categories listed in Article 9 UK GDPR (including data concerning health, SEND and ethnicity).

“Sub-processor” any third party appointed to process Personal Data on behalf of the Processor related to this Agreement.

Terms not defined above (Data Processor, Data Subject, Data Protection Officer, Processing, Personal Data, GDPR, etc.) have the meanings given in the Data Protection Legislation.

1.3 In the event of any inconsistency between this Agreement and the data protection provisions of the Processor's standard Terms and Conditions, this Agreement shall prevail. The standard Terms and Conditions shall govern all other aspects of the relationship (payment, termination, liability, access to the Services).

2 Roles and basis for processing and sharing

2.1 Each party will comply with all applicable requirements of the Data Protection Legislation. This Agreement is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Legislation.

2.2 The parties acknowledge that: (a) the Processor is the Data Processor of Personal Data it processes on behalf of the School and, from the LA Activation Date, on behalf of the LA; and (b) the School and the LA are each separate, independent Data Controllers, each determining the purposes and means of its own processing. They are NOT joint controllers.

2.3 In respect of the Shared Personal Data, the School acts as the disclosing Controller and the LA as the receiving Controller (see Annex 4); each is independently responsible for its own compliance once it holds the data.

2.4 The details of the processing are set out in Annex 1 (processing by the Processor for each Controller) and Annex 4 (one-way sharing from the School to the LA, effective only from the LA Activation Date).

PART A - Processing (Applicaa as Processor)

The following obligations of the Processor apply in respect of each Controller's Personal Data. "The relevant Controller" means the School or, from the LA Activation Date, the LA, as applicable to the data concerned.

3 Obligations of the Processor

3.1 The Processor shall only process Personal Data on behalf of the relevant Controller in accordance with the written instructions provided and as set out in Annex 1. If required to do otherwise by law it will promptly notify the relevant Controller before processing, unless prohibited by law.

3.2 The Processor shall provide reasonable assistance to each Controller in the preparation of any data protection impact assessment required prior to processing.

3.3 The Processor will maintain complete and accurate records of any processing of Personal Data it carries out on behalf of each Controller.

3.4 If the Processor receives any complaint, notice or communication relating to the processing or sharing of Personal Data or to any party's compliance, it shall promptly notify the relevant Controller(s) and provide full cooperation and assistance.

3.5 Taking into account the nature of the Personal Data, the harm that might arise, the state of technological development and the cost of implementation, the Processor shall ensure it has appropriate technical and organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction, alteration, unauthorised disclosure of, or access to, the Personal Data. In particular the Processor shall, as appropriate: pseudonymise and encrypt the Personal Data; ensure ongoing confidentiality, integrity, availability and resilience of systems; restore availability and access in a timely manner after an incident; and regularly test the effectiveness of those measures.

3.6 The Processor shall immediately inform the relevant Controller if any Personal Data is lost, destroyed, damaged, corrupted or becomes unusable, and will restore it at its own expense.

3.7 The Processor shall notify the relevant Controller immediately if it becomes aware of any (a) accidental, unauthorised or unlawful processing of Personal Data, or (b) Personal Data Breach, and shall comply with all reasonable requests in dealing with it. In any event notification shall be made in time to enable the relevant Controller to meet its own 72-hour ICO reporting duty.

3.7.1 On becoming aware of any matter in (a) or (b) the Processor shall provide: a description of its nature, including the categories and approximate number of Data Subjects and records concerned; the likely consequences; and the measures taken or proposed to address it and mitigate its effects.

3.8 The Processor shall cooperate with the relevant Controller and take reasonable steps as directed to assist in the investigation, mitigation and remediation of each Data Loss Event or Personal Data Breach.

3.9 On termination, or on request by a Controller, the Processor shall cease processing that Controller's Personal Data and return or securely destroy it (as instructed) and certify this within 30 days (extendable to 60+ by agreement). This does not apply to the company-wide encrypted backup of the entire cloud database, held for two years, not normally accessible to Applicaa staff and from which individual records cannot be deleted - ruled to conform to UK GDPR by the ICO (storage-limitation guidance).

3.10 A Controller may, by written notice from its Data Protection Officer, require the Processor to return a complete copy of that Controller's data in a reasonably specified medium at a reasonable cost.

3.11 A Controller may, by written notice from its Data Protection Officer, require the Processor to delete and procure deletion of all copies of that Controller's data. Exercising this right does not constitute termination unless the termination procedure is followed.

3.12 The Processor and its Sub-processors may retain a Controller's data to the extent required by law, ensuring confidentiality and processing only as necessary. The Processor may use anonymised usage information to monitor the Services and may access data to provide support, maintenance and to audit use of the Services.

4 Transfers outside the UK / EEA

4.1 The Processor shall not transfer Personal Data outside the UK or EEA unless: appropriate safeguards are in place; the transfer is to a country covered by UK adequacy or an Article 49 UK GDPR derogation applies; Data Subjects have enforceable rights and effective remedies; an adequate level of protection is provided; the Processor complies with the relevant Controller's advance instructions; and the Processor first informs the relevant Controller. A DPIA will be required in the first instance.

5 Processor's Personnel

5.1 Access to Personal Data is limited to Personnel who need it to meet the Processor's obligations.

5.2 The Processor shall ensure all Personnel are aware of their duties under the Data Protection Legislation and this Agreement; are informed of the confidential nature of the data; are subject to confidentiality undertakings; and have undertaken adequate data-protection training.

6 Rights of Data Subjects

6.1 The Processor shall notify the relevant Controller immediately if it or a Sub-processor receives a subject access request; a request to rectify, block or erase; a third-party request for disclosure required by law; or becomes aware of a Data Loss Event.

6.2 The Processor shall provide each Controller with full co-operation and assistance in relation to any such request.

6.3 Where a request concerns the Shared Personal Data, the Processor shall route it to, and assist, the Controller responsible under clause S7.

6.4 The Processor shall not disclose Personal Data to any Data Subject or third party other than at the request of the relevant Controller or as provided by this Agreement.

7 Rights of the Controllers (audit)

7.1 The Processor will make available all information necessary for each Controller to demonstrate UK GDPR compliance and allow for and contribute to audits, including inspections, conducted by that Controller or a mandated auditor, per clause 7.2.

7.2 A Controller may, on reasonable notice, inspect facilities, equipment, documents and electronic data relating to the processing, within business hours, minimising disruption.

7.3 A Controller may require the Processor to cease using named Personnel for handling that Controller's data where an inspection reasonably shows they are causing a breach.

7.4 A Controller may make reasonable objections to changes or appointments of Sub-processor.

8 Warranties

8.1 The Processor warrants that it will process and share the Personal Data in compliance with the Data Protection Legislation and all applicable law; take appropriate technical and organisational measures; and protect against unauthorised or unlawful processing and accidental loss or damage.

9 Indemnity

9.1 The Processor agrees to indemnify each Controller against all costs, claims, damages and expenses incurred due to any failure by the Processor or its Personnel to comply with the Data Protection Legislation or its obligations under this Agreement.

9.2 The Processor shall maintain insurance to cover any payment required under clause 9.1.

10 Appointment of Sub-processors

10.1 The Processor shall not sub-contract processing without the relevant Controller's prior authorisation. As at each party's Commencement Date that party authorises the Sub-processors in Annex 3 and replacements appointed under clause 10.2.

10.2 The Processor may authorise a Sub-processor only if it supplies full details; gives the relevant Controller 5 business days to object; enters a written agreement on equivalent terms; and ensures the Sub-processor ceases processing on termination.

10.3 The Processor remains fully liable for the acts and omissions of its Sub-processors.

10.4 The Processor shall consider all reasonable objections; 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 Processor's standard Terms and Conditions apply. In addition the Processor shall have no liability for loss, interception or corruption of data except to the extent caused by the negligence or breach of the Processor or a Sub-processor, or resulting from a telecommunications provider's default.

PART B - Local Authority destination tracking (effective only upon LA accession)

S0.1 Part B has no effect unless and until the LA has accepted this Agreement in accordance with clause 16. By accepting this Agreement the School authorises the sharing described in this Part and in Annex 4; that sharing commences only on or after the LA Activation Date and continues only while the LA participates in a destination-tracking programme. Applicaa will notify the School through the platform when the LA's acceptance takes effect.

From the LA Activation Date, this Part governs the one-way sharing of the Shared Personal Data from the School to the LA as independent Controllers. Applicaa provides the platform through which the sharing occurs but is not a Controller of this sharing.

S1 Shared Personal Data and Agreed Purposes

S1.1 The School shall make available to the LA, and the LA shall receive, the Shared Personal Data described in Annex 4 (post-16 destination/NEET and attendance data), solely for the Agreed Purposes.

S1.2 Each Controller shall process the Shared Personal Data only for the Agreed Purposes and shall not process it in a way incompatible with those purposes.

S2 Status of the Controllers

S2.1 The School and the LA are separate, independent Controllers of the Shared Personal Data. Neither is the other's processor and they are not joint controllers. The sharing is a single controller-to-controller disclosure from the School to the LA, with its own lawful basis and, where relevant, Article 9 condition.

S3 Lawful basis

S3.1 Each Controller shall ensure it has a valid Article 6 UK GDPR basis for its processing of the Shared Personal Data and shall maintain records of that basis.

S3.2 Each Controller shall ensure the sharing is fair and transparent to Data Subjects, including through its privacy notice.

S4 Special Category Data

S4.1 Where the Shared Personal Data includes Special Category Data (e.g. SEND, health), each Controller shall identify and record a condition under Article 9 UK GDPR and the associated condition in Schedule 1 to the Data Protection Act 2018.

S5 Purpose limitation and onward sharing

S5.1 The LA shall not use the Shared Personal Data for any purpose other than the Agreed Purposes.

S5.2 Neither Controller shall disclose the Shared Personal Data to any person who is not a Permitted Recipient, except (a) as required by law, or (b) onward disclosure strictly within, and necessary for, its statutory functions and subject to equivalent protections.

S6 Data quality, minimisation and retention

S6.1 The School, as the disclosing Controller, shall take reasonable steps to ensure the Shared Personal Data is accurate at the point of sharing. The Controllers shall share only the minimum data necessary for the Agreed Purposes.

S6.2 Each Controller shall retain the Shared Personal Data only for as long as necessary for the Agreed Purposes and shall then securely delete or return it.

S7 Data subject rights

S7.1 Each Controller is responsible for handling requests by Data Subjects in respect of the data it holds. Where a request concerns data held by both, the Controllers shall cooperate and respond without undue delay, and the Processor shall assist under clause 6.

S8 Controller-to-controller breach notification

S8.1 If a Controller becomes aware of a Personal Data Breach affecting the Shared Personal Data, it shall notify the other Controller without undue delay and, where feasible, within 24 hours, and the Controllers shall cooperate on investigation, mitigation, Data Subject notification and any ICO report. This is in addition to the Processor's obligations under clause 3.7.

S9 Security of shared data held by the LA

S9.1 The LA, as the receiving Controller, shall implement appropriate technical and organisational measures to protect the Shared Personal Data it holds, at least equivalent to those required of the Processor under clause 3.5, and shall restrict access to Permitted Recipients on a need-to-know basis.

S10 Duration and deactivation of Part B

S10.1 Part B is active from the LA Activation Date and remains active while the LA participates in a destination-tracking programme. If the LA ceases to participate, or the LA's accession is terminated, Part B deactivates: sharing ceases and the LA shall delete or return the Shared Personal Data it holds in accordance with clause S6.2. Deactivation of Part B does not affect Part A or the remainder of this Agreement between the School and the Processor.

General

12 Review

12.1 Any amendment to this Agreement becomes effective when accepted in accordance with clause 16, and the Agreement may be reviewed to ensure continued compliance with the Data Protection Legislation and ICO guidance.

13 Third party rights

13.1 No person who is not a party to this Agreement shall have any rights under it, whether under the Contracts (Rights of Third Parties) Act 1999 or otherwise, save that each Controller may enforce the provisions of Part B against the other from the LA Activation Date.

14 Governing law

14.1 This Agreement and any dispute arising out of or in connection with it shall be governed by the laws of England and Wales, and the parties submit to the exclusive jurisdiction of the courts of England and Wales.

15 AI-assisted processing

Where the Processor provides AI-assisted features, the Processor shall: process a Controller's Personal Data only as needed to respond to the user's request; act only on the relevant Controller's documented instructions, including where a user works with special category data; ensure the AI sub-processor is bound by obligations consistent with Article 28 UK GDPR; 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; process such data within the UK/EU/EEA; and not use the assistant to make solely-automated decisions producing legal or similarly significant effects about an individual (Article 22 UK GDPR).

16 Acceptance and records (electronic acceptance)

16.1 Acceptance. This Agreement is accepted electronically; no wet signature is required. A School accepts this Agreement by an authorised user confirming acceptance in the Applicaa platform at onboarding or, where the School is already a customer when a new version is issued, in accordance with clause 16.4. The LA accepts this Agreement by an authorised officer confirming acceptance in the Applicaa platform, and its acceptance operates as its accession to this Agreement as Controller B; the LA's accession always requires affirmative acceptance and cannot take effect by notice. Each party accepts its own copy of the same version; a joint signing session is not required. Acceptance constitutes a binding agreement with the same effect as a signature.

16.2 Authority. Each Controller confirms that the individual accepting on its behalf is authorised to bind that organisation. Acceptance shall be given by an appropriate role - for the School, its DPO, headteacher or a data manager with delegated authority; for the LA, a named officer with authority over its data-sharing arrangements.

16.3 Record. Applicaa shall maintain an auditable Acceptance Record for each party capturing the accepting individual's name and role, the organisation, the date and time, the version accepted, and the account used. Where a version takes effect by notice under clause 16.4, Applicaa shall instead record the version concerned, the account notified, the date the notice was given and the date the version took effect. That record is evidence of acceptance.

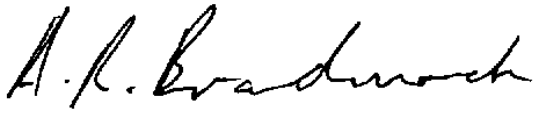
16.4 Versioning and updates by notice. Each version of this Agreement is uniquely identified. Where Applicaa issues a new version, it will notify each affected party through the Applicaa platform and make the new version available to read. The new version takes effect for that party thirty (30) days after the notice is given, and the party's continued use of the Services after that date constitutes its acceptance of that version; the previous version governs until that date. A party that does not wish to accept a new version may terminate in accordance with the Processor's standard Terms and Conditions. This clause does not apply to the LA's accession under clause 16.1.

16.5 Controller compliance confirmations. In respect of any processing it carries out under Part B, each Controller confirms that, before any Shared Personal Data is shared and for as long as the sharing continues: (a) it has identified and documented the applicable Article 6 UK GDPR lawful basis; (b) where Special Category Data is processed, it has identified and documented the applicable Article 9 UK GDPR and Data Protection Act 2018 Schedule 1 condition; (c) where the applicable Schedule 1 condition requires an Appropriate Policy Document, an appropriate and current document is in place; (d) it is satisfied that the sharing described in this Agreement is reflected in the privacy information made available to Data Subjects, including through the privacy notices Applicaa presents to schools, students and applicants; and (e) it will keep these matters under review while participating in the data-sharing arrangement.

17 Prior agreements

17.1 With effect from the School's Commencement Date, this Agreement replaces any earlier data processing agreement between the School and the Processor. Processing carried out before that date remains governed by the agreement in force at the time.

Signed: For and on behalf of Applicaa Ltd:



Name: Andrew Bradnock
Position: DPO
Date: 26th August 2026 (effective 7th October 2026)

Signed: For and on behalf of:

Name:
Position:
Date:

Annex 1 - Processing, Personal Data and Data Subjects

Part 1 - Processing carried out by Applicaa for the School

Subject matter	Student data including admissions and student bursary data.
Duration	For the School's subscription; deleted on termination (subject to clause 3.9 backup).
Nature and purpose	To help the School process admissions and enrolment applications efficiently, including the AI Assistant, and, where the School's Local Authority participates in a destination-tracking programme, provision of destination and attendance data to that Local Authority under Part B.
Lawful basis	State schools: public task. Independent schools: performance of a contract.
Type of Personal Data	Student personal details and any data configured by the School, which may include special category data (health/medical, SEND, ethnicity) and family financial data.
Categories of Data Subject	Students, parents/guardians and school staff.
Return / destruction	The School can export data at any time; on termination the data is removed and destroyed (subject to clause 3.9).
Storage location	Amazon Web Services (UK).

Part 2 - Processing carried out by Applicaa for the Local Authority (from the LA Activation Date)

Subject matter	Post-16 destination and participation data and attendance data for young people in the LA area, across the LA's participating schools.
Duration	For the LA's participation in the programme; deleted per clause S6.2.
Nature and purpose	To host and display school-provided destination/NEET and attendance data to authorised LA users for the Agreed Purposes. Applicaa acts as Processor for the LA in respect of the LA's use of this data in the dashboard.
Lawful basis	Public task - the LA's statutory functions: Education and Skills Act 2008 (participation/NEET); statutory attendance framework (attendance).
Type of Personal Data	Student identifiers, current school, application/destination status, attendance data; may include Special Category Data (e.g. SEND).
Categories of Data Subject	Children and young people in the LA area.
Cross-school access	Authorised LA users may access data across the LA's participating schools, scoped strictly to the Agreed Purposes.
Storage location	Amazon Web Services (UK).

Applicaa contact: Antony Wambua, COO - antony@applicaa.com - 020 4 538 1630 - Wyevale Business Park, King's Acre, Hereford, HR4 7BS.

Annex 2 - Security measures adopted by the Processor

Item	Provider response
Physical access controls	No physical access to the data. All servers are cloud-hosted and secured by Amazon Web Services.
System access controls	Servers (web, database) can only be accessed by the lead technical member; IP address restricted in the UK; encrypted connections.
Data access controls	Access to student data is role-based and restricted to authorised users. School staff access their own school's data; authorised Local Authority users may access data across the LA's participating schools strictly for the Agreed Purposes. Each user has permissions scoped to the data sections they need.
Transmission controls	No data is transferred outside the UK/EEA save as permitted under clause 4.
Input controls	Student details are input by the student, parent and school staff using registered accounts at Applicaa.
Data backups	Amazon RDS and Amazon S3 backups.
Data segregation	Servers are located across multiple availability zones (at least three in London) for resilience.

Personnel checks / training	Applicaa staff are trained regularly on data security (including GDPR), data processing and security procedures.

Annex 3 - Sub-processors

All sub-processors have their GDPR compliance checked annually 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")	EU	Data remains in EU/EEA (UK adequacy); not retained; not used for training.
Esendex	SMS messaging	UK	
Google Workspace	Internal email system	UK	
HubSpot	Customer database and support ticket logging	USA	Safeguarded by SCCs.
Postcode Look-Ups	Address lookup	UK	
SendGrid / Twilio	SMTP mail forwarding	USA	Safeguarded by SCCs.
Slack	Internal messaging and collaboration	USA	Safeguarded by SCCs.
Stripe	Payment processing	USA	Safeguarded by SCCs.
Xero	Accounting	USA	Safeguarded by SCCs.
Zoom	Video conferencing	USA	Safeguarded by SCCs.

Additionally, some contractor staff operate outside the EEA; all are subject to the same Security and Acceptable Usage policies and are protected by UK GDPR-compliant International Data Transfer Agreements.

Annex 4 - Data Sharing Schedule (Part B - applies only from the LA Activation Date)

Direction: ONE-WAY (School → LA only).

Data shared - School → LA	Student identifiers (e.g. UPN, name, DOB), current school, post-16 applications and status, destination / intended destination, NEET-risk indicators, and attendance data. May include SEND status.
Agreed Purposes	Post-16 destination tracking; identification and support of NEET / at-risk young people; September Guarantee / statutory participation; attendance monitoring in support of the above.
Recipients	At the LA: named authorised officers with a role-based need (Permitted Recipients only).

Frequency / method	Continuous, via the Applicaa platform, scoped to the LA's participating schools and current admissions year(s).
Retention	Each party retains the Shared Personal Data only for as long as necessary to carry out its duties for the Agreed Purposes, in line with clause S6.2.
Special category data	SEND / health where present - Article 9 condition per clause S4.

Change history

V2.5 (11 June 2026): updated signature section; updated for the Emma AI assistant.

V3.0 (26 August 2026): added provision for Local Authority destination tracking. The School's Local Authority is identified by reference to the Department for Education's Get Information About Schools register and becomes a party to this Agreement upon its own acceptance. New Part B governs the one-way sharing of destination, NEET and attendance data from the School to the Local Authority, including purpose limitation, lawful basis, special category safeguards, retention and breach notification, and takes effect only from the LA Activation Date. Added Annex 1 Part 2 (Local Authority processing) and Annex 4 (Data Sharing Schedule); updated Annex 2 data access controls; confirmed electronic acceptance and records (clause 16); this Agreement supersedes any earlier data processing agreement between the School and Applicaa (clause 17).