



PlannedQuest Data Privacy Addendum

Version 2.1 · Effective October 6, 2026 · plannedquest.com/legal/data-privacy-addendum

This Data Privacy Addendum ("DPA") is part of the PlannedQuest Subscription Agreement between **PlannedQuest Inc.** ("PlannedQuest", "we") and the customer named in the Order ("Customer"). It protects the data of the school, district, or program whose students use the Service (the "Institution"). When the Customer is an organization, the Customer is the Institution. When the Customer is an educator who bought an Educator Pilot, the Institution is the school, district, or program the educator named at purchase, and Section 3 applies.

If this DPA conflicts with the Subscription Agreement, this DPA controls as to Institutional Data. A data privacy agreement both parties have signed, including a state or consortium form, controls over this DPA.

In plain language. The school owns its students' data. We use it only to run PlannedQuest for the school. We never sell it, never advertise with it, and never use it to train AI. We tell the school within 72 hours if something goes wrong, and we delete the data when the school asks.

1. Definitions

- **Institutional Data:** data the Institution or its Authorized Users provide to the Service, or that the Service generates about them, including Student Data.
- **Student Data:** personally identifiable information about a student, including education records under FERPA and pupil records under state law.
- **Pupil-Generated Content:** material a student creates in the Service, including saved careers, colleges and programs; plans; portfolio entries; goals; reflections; and free-text responses.
- **Authorized Users:** students, staff, and linked parents and guardians the Institution permits to use the Service.
- **Personal Data Breach:** unauthorized access to, or acquisition, use, disclosure, alteration, or destruction of, Institutional Data.

2. Roles and ownership

2.1 The Institution is in control. The Institution owns and controls Institutional Data. PlannedQuest processes it **only on the Institution's documented instructions**, which are this DPA and the Subscription Agreement. PlannedQuest does not decide the purposes or means of processing Institutional Data, and any change to them requires the Institution's written instruction.

2.2 Ownership survives. Pupil records remain the property of and under the control of the Institution. That survives any change of control, insolvency, or end of our business: Institutional Data is not a PlannedQuest asset and cannot be sold or transferred as one. If we plan to stop operating, we give the Institution at least **90 days' written notice** to export its data.

2.3 What we process. The nature and purpose of processing, the categories of data, and its duration are described in **Annex A**. Annex A is written to be read. It includes sensitive categories that a student may choose to share, and it describes who can see them.

3. Educator pilots

This Section applies when an educator buys an Educator Pilot for their own use.

3.1 Authorization. The educator confirms at purchase that their use of PlannedQuest with students follows the Institution's technology and student-data policies, or has been approved by an administrator with authority. The Institution's authorization is given for the use and benefit of the Institution, and PlannedQuest uses Institutional Data only as this DPA allows.

3.2 Notice to the Institution. Where the educator gives us an administrator's email address, we send that administrator this DPA and a notice of what the Service collects. Any administrator of the Institution may contact **privacy@plannedquest.com** at any time to ask questions, review the pilot, or exercise the Institution's rights under this DPA.

3.3 The Institution decides. The Institution, not the educator and not PlannedQuest, decides what happens to its students' data. If the Institution tells us it does not authorize the pilot, we stop collecting data from its students and, at the Institution's choice, return or delete their data under Section 9. The educator receives a pro-rata refund under the Subscription Agreement.

3.4 Moving a pilot into a school license. If the Institution later buys a School License, the educator may move the pilot's students and their work into the Institution's account. This is a transfer within the same Institution's data, not a disclosure to a third party.

4. Our obligations

PlannedQuest will:

1. process Institutional Data **only to provide the Service**, and for no other purpose;
2. **not sell Student Data, use it for targeted advertising, build a profile of a student for any non-educational purpose, or use it to train an artificial intelligence model;**
3. limit access to personnel who need it to provide the Service, under confidentiality obligations;
4. maintain the safeguards in **Annex C**, and not materially reduce them during the term;
5. help the Institution respond to requests under Section 7;
6. notify the Institution of a Personal Data Breach under Section 6; and
7. delete or return Institutional Data under Section 9.

4.1 No AI. The Service has no generative AI feature and sends no Student Data to any AI model provider. We use an AI image service in an internal tool to draw career illustrations; it receives an occupation title and never any user, student, or Institutional Data.

4.2 No advertising. The Service shows no advertising to students.

5. Subprocessors

5.1 The list. Our current subprocessors, with the purpose and location of each, are published on our privacy page at plannedquest.com/privacy. **That published list is Annex B and is incorporated here by reference**, so the two cannot drift apart.

5.2 Their obligations. Each subprocessor is bound by a written contract that requires it to implement and maintain reasonable security measures protecting Institutional Data, restricts its use of the data to providing its service to us, and prohibits onward disclosure. We remain responsible for their acts and omissions.

5.3 Changes. We update the published list **before** a new subprocessor processes Student Data, and give the Institution's named contact written notice before a material change to the list or to our privacy policy. The Institution may object in writing within 30 days. **If we cannot resolve the objection within 30 days, the Institution may end the affected services without penalty and receive a pro-rata refund.**

6. Personal Data Breach

6.1 Notice. We notify the Institution's named contact in writing **promptly on discovering** a Personal Data Breach affecting Institutional Data, and in any event **within 72 hours of discovery**. The notice states what happened, the categories and approximate number of records and people affected, the likely consequences, and what we are doing about it. We update it as we learn more. Where a law applicable to the Institution sets a shorter deadline, we meet it.

6.2 Notifying families. The Institution, as the educational agency, notifies affected parents, guardians, and eligible students. We support that at no charge by providing, as fast as the investigation allows, the list of affected individuals and the data involved for each, a factual description the Institution can use in its own notice, and one named contact for the incident. If the Institution directs us in writing, we send notices on its behalf using content it approves.

6.3 Regulators. Where a law requires PlannedQuest itself to notify a state attorney general or other regulator, we do so, in addition to notifying the Institution.

6.4 Costs. Where a breach is caused by PlannedQuest, we bear the reasonable cost of notifying affected individuals and regulators, of credit monitoring where offered, and of the Institution's reasonable legal review of its notice duties. Where a breach is caused by the Institution, the Institution bears those costs. Where responsibility is shared, costs are shared in proportion.

7. Access, correction, and student work

7.1 Requests. The Institution answers requests from students, parents, guardians, and eligible students. We help within **10 business days** of a forwarded request.

7.2 Review and correction. A parent, guardian, or eligible student may review the personal information the Service holds about the student and have errors corrected. Institution staff can view and change much of it in the Service; where they cannot, the Institution forwards the request and we make the correction within the period in 7.1.

7.3 Student work. On the Institution's request, we provide a student's Pupil-Generated Content in a structured, machine-readable format, at no charge, so the student can keep a copy independent of the Service. The export covers saved careers, colleges, and programs; plans; portfolio entries; goals; reflections; assessment and survey responses; network contacts and notes; and free-text responses.

7.4 What is not self-service yet. A student or parent cannot yet download their own data from inside the Service. Requests go to the Institution, or to privacy@plannedquest.com, and we fulfil them within the period in 7.1. A student's message export covers messages the student sent; messages they received belong to another user's conversation. We will tell the Institution when self-service export ships.

8. FERPA, COPPA, and student privacy

8.1 FERPA. PlannedQuest acts as a **school official with a legitimate educational interest** under 34 C.F.R. 99.31(a)(1)(i)(B), under the Institution's direct control with respect to the use and maintenance of education records. We do not redisclose education records except on the Institution's instruction or as the law requires. **PlannedQuest agrees to comply with FERPA** with respect to Institutional Data.

8.2 Annual notice. The Institution includes providers like PlannedQuest within its criteria for school officials in its annual FERPA notification.

8.3 COPPA. Where the Institution provides accounts to students under 13, it authorizes the collection of their personal information for the educational purpose of the Service, for the use and benefit of the Institution and for no commercial purpose. **Complying with the Children's Online Privacy Protection Act is PlannedQuest's responsibility, not the Institution's.** The Institution may, on a parent's request, review the child's information, have it deleted, and have its collection stopped, and we act on that request.

8.4 De-identified data. Where we describe data as de-identified, we keep and use it only in de-identified form, do not attempt to re-identify it, and require the same of anyone we share it with.

8.5 Legal demands. We disclose Institutional Data in response to a legal demand only if it is valid, and we notify the Institution first where the law allows.

8.6 Responsible individual. PlannedQuest designates a named individual accountable for the security and confidentiality of Institutional Data, identified to the Institution on request. Personnel given access to Student Data are trained on the federal and state laws that protect it before access is granted, and annually after.

8.7 No binding of families. Nothing in this DPA or the Subscription Agreement binds a student or parent to any term, including any arbitration term.

9. Term, return, and deletion

9.1 Term. This DPA runs for as long as we process Institutional Data.

9.2 Export window. The Institution may ask for an export of its data during the term and for **60 days** after it ends. We deliver it **within 10 business days** of the request.

9.3 Deletion. At the Institution's choice, on termination or on written request, we delete or return Institutional Data **within 30 days**. **When the subscription ends, we do not retain pupil records**, except the records listed in 9.4, and we provide **written certification of deletion** on request.

For an individual user, deletion runs against one reviewed registry covering every store in our primary database keyed to a user. It permanently deletes the user's own records, removes their references from shared structures, and replaces their identifier with a non-identifying value in records shared with other people, so another user's record of a shared interaction is not destroyed. Records held outside that database, including imported roster rows, reference-database links, and billing records, are deleted on request as a separate step we perform.

9.4 What survives deletion.

- **Messages sent to other users** stay in those users' conversations, with the sender's name removed. The same applies to staff notes about other students and to content a user wrote for an organization.
- **A defined set of audit, security, and safety records is retained**, each for a documented reason, including records the Institution is itself required to keep: authentication and security audit logs, organization audit logs, data-export and FERPA disclosure logs, account-merge and impersonation records, content-moderation and safety cases, and grade-promotion records.
- **The security record of a deletion** includes a snapshot of the user's primary account record at the time of deletion, kept **for one year** so a mistaken or malicious deletion can be investigated.
- **Encrypted backups** keep deleted data until they expire on their normal schedule; we do not extract it from them.

9.5 Roster imports. When the Institution imports a roster, the Service keeps the rows it received so a later sync can be reconciled. Deleting a user removes the rows tied to that user. Remaining organization-level rows are removed on request under 9.6. The Institution may leave the optional demographics file out of its import. **Passwords and credential columns in a roster file are never stored.**

9.6 Organization deletion is performed by PlannedQuest on request and confirmed in writing.

9.7 Requests from families. Where the Institution has no policy of its own for a parent, guardian, or eligible student to request deletion, we honour such a request made directly to us within the period in 9.3, and tell the Institution.

10. Security

10.1 Safeguards. The measures in **Annex C** apply, and we will not materially reduce them during the term. Annex C states what is not yet in place as well as what is.

10.2 Written security program. PlannedQuest maintains a **written information security program** covering the security, confidentiality, and integrity of Institutional Data, with administrative, technical, and physical safeguards suited to our size and the sensitivity of the data. We provide it to the Institution on request, give notice before a material change to it, and confirm it exists so the Institution can meet any disclosure duty of its own.

10.3 Retention. We keep Institutional Data only as long as needed to provide the Service to the Institution, under the retention periods in Annex A and Section 9.

11. Audit

11.1 Information. On written request, we give the Institution the information it needs to verify that we meet this DPA, including our security documentation and completed security questionnaires, at no charge. We may decline a request that is repetitive, disproportionate, or made in bad faith, with our reasons in writing.

11.2 Assessment. The Institution, someone it designates, or an independent assessor may assess our policies and measures on reasonable notice, no more than once in any 12 months unless there has been a confirmed Personal Data Breach.

11.3 On-site audit. An on-site audit is available where the law requires it, or after a confirmed Personal Data Breach, with scope and dates agreed in advance. The Institution bears the reasonable costs, and results are confidential.

12. Data location

12.1 Storage. Institutional Data at rest is stored in the **United States**, including database backups.

12.2 Processing. Our application servers, website, file storage, sign-in, email, caching, and payments run in United States regions. Database traffic passes through one relay host in Hillsboro, Oregon, operated on infrastructure from **Hetzner Online GmbH, a company based in Germany**. The relay carries only encrypted traffic, cannot read Institutional Data, and remains in the United States.

12.3 Logs. Application logs, which can contain account identifiers, IP addresses, and requested pages, go to the log service named on the published subprocessor list, at the location stated there.

12.4 No transfer abroad. We do not transfer Institutional Data outside the United States except as stated in this Section. Moving storage or processing outside the United States is a material change that requires prior notice under 5.3.

13. General

13.1 Liability. Liability limits and indemnities are in the Subscription Agreement and apply to this DPA, except as stated in 13.5.

13.2 Governing law. This DPA is governed by the law of the state where the Institution is located, without regard to conflict-of-laws rules.

13.3 Severability. If a provision is invalid, the rest stays in force and that provision is reformed only as much as needed to make it enforceable.

13.4 Publication. The Institution may publish this DPA where the law requires it, redacting anything whose publication would weaken the security of Institutional Data.

13.5 Remedies. For **intentional or grossly negligent** noncompliance with this DPA, the Institution may terminate the Subscription Agreement on written notice without penalty or cure period, and recover monetary damages caused by it. This remedy is in addition to any other available at law and **is not limited by any liability cap in the Subscription Agreement.**

13.6 Notices. Notices go to each party's named contact. Our privacy contact is privacy@plannedquest.com; security reports go to security@plannedquest.com.

13.7 State law. Where the law of the Institution's state requires a provision this DPA does not contain, we will sign that state's standard student data privacy agreement on request, including the Student Data Privacy Consortium National Data Privacy Agreement and its state versions, and that agreement controls.

Annex A: Details of processing

Item	Description
Subject matter	A college and career readiness platform
Duration	The term of the Subscription Agreement, plus the windows in Section 9
Nature and purpose	Hosting, storing, displaying, and analysing Institutional Data so students can explore careers and education pathways, build plans, and share them with the educators and families who support them
Data subjects	Students; Institution staff; linked parents and guardians

Categories of Institutional Data

- **Identity and contact:** name, preferred name, email address, school-assigned identifier, username, phone number where supplied, pronouns, grade level, school, and organization.
- **Roster and enrollment:** roster import is by OneRoster CSV file. Where the Institution supplies the **optional** demographics file, the Service stores all thirteen OneRoster demographic fields (date of birth;

sex; race and ethnicity indicators; country, state, and city of birth; and public-school residence status). Only sex is read back by the Service. The Institution may leave the file out.

- **Gradebook outcomes:** where the Institution supplies line-item and result files, the Service stores assignment definitions and per-student scores, status, late and missing flags, and teacher comments, used in two staff reports. The Institution may leave these out.
- **Student work and choices:** saved careers, colleges, and programs; plans and plan notes; portfolio entries; goals; assessment and survey responses; and free-text responses.
- **Preferences:** including college-search preferences such as religious affiliation and institution type, household income **band**, home state, and ZIP code.
- **Location:** where a student uses "use my location", precise device coordinates may be stored in a saved search.
- **Staff-authored records:** counselor notes (not visible to the student by default), notes on individual situation items, and content-moderation cases, which can include self-harm and harassment reports and store the flagged content.
- **Derived indicators:** readiness and engagement indicators computed from activity in the Service.
- **Technical:** IP address, browser, referrer, session identifier, pages requested, and timestamps, kept **18 months**; search text, kept **90 days**.

Sensitive categories a student may choose to share. The Service offers a "Your Situation" checklist. **The Institution may make it optional, turn it off, or hide individual items.** Choosing items is voluntary and skippable. Items depend on the student's grade:

- **From grade 6:** disability, learning differences, and accommodations; mental health; chronic illness; housing instability or an unsafe home; food insecurity; foster care, current or former; caregiving and childcare; limited family support; transportation and phone costs; lack of reliable internet, a computer, or a place to study; needing to work while in school; concern about education costs; concern that financial aid will not be enough.
- **From grade 9:** pregnancy or expecting a child; raising children; justice-system involvement; first-generation status; military-connected status; international-student status; needing to support oneself soon.
- **From grade 11:** health insurance access; not having a bank account; uncertainty about financial systems, college supports, or return on investment.
- **A free-text field** where the student can describe a circumstance in their own words.
- **Never collected:** immigration or residency status and English-learner status are blocked by the server, and no setting can turn them on. The Service has no IEP, 504, special-education, or free-and-reduced-lunch field.
- Where a student's grade is missing or unreadable, the Service shows the full adult set of items. Institutions should make sure roster rows carry a grade.

Who can see sensitive categories. Situation choices, including the free-text entry, are visible to the student's teachers, coaches, counselors, and district administrators; can be **searched by category** by

staff; and can be **exported to CSV and PDF** with student names. They are not sent to linked parents' home view. Where the Service has built a plan for the student, **up to three situation items appear in the plan's "Considerations for you" section, which a linked parent can see by default.** The Institution can turn this off for its whole organization, and should decide this during setup.

Annex B: Subprocessors

The authorized subprocessors are those published, with purpose and location, at **plannedquest.com/privacy**. That list is incorporated into this DPA by reference and changes only as Section 5.3 allows.

Annex C: Technical and organizational measures

In place

- **Encryption in transit:** TLS on all application traffic, with HSTS on the web and API. The primary database refuses unencrypted connections. The reference database is reached through a managed connector using mutual TLS that refuses to fall back to a direct connection.
- **Encryption at rest:** provider-managed encryption on both databases.
- **Network:** application traffic to the primary database leaves through one hardened relay with a fixed address, and the database accepts only that address and one administrative address. The application will not run if the relay is unavailable.
- **Access control:** least-privilege, role-based access enforced on the server, with exact role checks for privileged actions.
- **Audit logging:** a security audit log of sign-in, token, role-change, and impersonation events, kept one year and readable only by platform administrators.
- **Code security:** secret scanning on every change, a weekly full-history rescan, and weekly dependency-update scanning.
- **Backups:** continuous backup with point-in-time recovery on the primary database; daily backups kept seven days on the reference database.
- **Documented plans:** information security, incident response, disaster recovery, and business continuity.
- **Vulnerability reporting:** a published security contact (security@plannedquest.com) with a five-business-day response commitment.

Not yet in place, stated rather than omitted

- **Multi-factor sign-in is not available in the product** for any role. Where the Institution connects its own sign-in provider, that provider's requirements apply. We require multi-factor sign-in on our own hosting and vendor accounts.
- **No SOC 2 report** has been issued and **no third-party penetration test** has been performed.
- **Disaster recovery and backup restore testing:** a disaster recovery tabletop exercise and a backup restore test were completed in August 2026; incident response exercises are run annually. Our recovery

objectives are targets confirmed by that test.

- **No self-service data export or deletion** (see 7.4).
- **No public status page.**

More detail on each item, including planned dates, is in our security documentation, available to the Institution under 11.1.

PlannedQuest Inc. · privacy@plannedquest.com · security@plannedquest.com · support@plannedquest.com