Privacy Policy

Last Updated: June 10th, 2024

Welcome to the Privacy Policy of Maya Bialik LLC, doing business as QuestionWell AI. We provide teachers and school staff with online access to generative artificial intelligence tools through our website (collectively our "Services"). At QuestionWell, we value your privacy and safety.

This Privacy Policy explains how we gather, use, share, and handle your personally identifiable information (PII) when you use our Services.

What Data We Collect

a. Account Information. To sign in, you use Microsoft or Google, which provides us with your name and email address (“Login Info”). To see what personal information you have made available, you can check your google account.

b. Technologically Collected Information. Our servers, managed by Microsoft, gather some standard technical details about your device and the programs you use, like the type of internet browser, your operating system, and your IP address—a unique number given to your computer that changes and can show approximately your location. We collect this information each time you visit our website or log into your account. We collect data about how many people visit and use our services in order to improve the services we provide. The data is aggregated so we cannot use it to identify individuals. No data is shared or sold to third parties.

c. Cookies: We use cookies to keep track of ongoing sessions and see how people use our services. Cookies are tiny bits of data sent to your computer by a website, which help the site remember you, for example to keep you from being logged out. You can delete permanent cookies at any time through your browser's help section. This may affect how our website works for you, since some cookies are needed for it to work properly. The only cookies that aren’t necessary for the site to function simply track how visitors use our site to help us improve the user experience through anonymized and aggregated data. This data is not shared with or sold to anyone.

d. Information You Provide When Visiting Our Websites: You can visit our websites without an account or giving us any information. But, if you want to use certain services, we'll need some details from you. For instance, if you create an account in order to use the Services, you will be required to sign in with Google or Microsoft and thus share your name and email.

If you contact us by email for any reason, we'll collect your name and email address, along with any other information you include in your email, to reply to you. If you order any services that cost money, we'll need information for billing, which Stripe, a secure third-party processor, will handle.

How We Use the Data We Collect.

To summarize, we use your personal information to:

- Help you with your requests.
- Improve and secure our services.
- Follow the law.

Specifically at QuestionWell we use your information to:

- Recognize you when you use our services.
- Help set up and protect your account.
- Complete your requests.
- Make your experience better.
- Send you updates about service changes or security notices.
- Answer your questions and help with your requests.
- Send you newsletters, surveys, or information about new offers and upgrades (if you opt in).
- Follow relevant laws and respond to legal demands or court orders.
- Protect our rights and the rights of those we interact with.

No ads are displayed on this platform.

Aggregated and Anonymized Data

We also gather general data that does not personally identify you in order to improve our services. This data is turned into aggregated statistics and is completely anonymous and cannot be linked back to any person. We use this information to train our AI models and glean trends about how people generally use our services. We make sure all customer data is securely encrypted both at rest and in transit.

About third-party services:

- ## Google Analytics.

  We use third-party analytics tools like Google Analytics to understand how our users (aggregated and anonymized) use our website and services. These tools collect data to help improve your experience and fix any issues.
  For more: https://policies.google.com/technologies/partner-sites

- ## Open AI.

  We have opted OUT of allowing OpenAI to use the data they get from us to train their models. We use the Application Program Interface (API) of OpenAI to power our services. **Important notes from the API policy: "OpenAI will not use data submitted by customers via our API to train or improve our models, unless you explicitly decide to share your data with us for this purpose."**
  For more: https://openai.com/enterprise-privacy

- ## Microsoft Azure

  Microsoft uses and enables the use of industry-standard encrypted transport protocols, such as Transport Layer Security (TLS) and Internet Protocol Security (IPsec). All secrets such as encryption keys are properly secured in a secrets manager. All data is stored at a Microsoft data center on the east coast of the US. Microsoft defends your data through clearly defined and well-established response policies and processes, strong contractual commitments, and if necessary, the courts. All communication between users and our service is SSL encrypted according to industry best practices.

- ## Stripe

  For all financial transaction information we use Stripe, a trusted financial service. This way, we do not have to worry about storing your sensitive financial data. Stripe will not sell, retain, use or disclose Personal Data for any purpose other than for the specific purposes of performing the Services and to comply with Law. Stripe implements and maintains a written information security program and a data security incident management program that addresses how Stripe will manage a data security incident involving the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of, or access to, Personal Data.

  For more: https://stripe.com/privacy

- ### Browserless.io

  Browserless.io is used to fetch the contents of web pages for generating user content. The URLs that users enter into The Service may be transmitted to Browserless.io. No other information is transmitted to them.

  For more: https://www.browserless.io/privacy-policy/

- ### Google Authentication

  We use Google OAuth to authenticate users' identities so that we can provide them the services they need, and comply with Google's security recommendations. We do not process or store any plain-text client information and store tokens securely in an encrypted database. We never commit secrets, including Google OAuth secrets, to any code repositories. All secrets are stored in an encrypted secrets manager. When we no longer need access to a user's account or no longer need access to permissions that a user previously granted, their tokens are revoked. After the tokens are revoked, they are deleted permanently from the system.
  For more: https://policies.google.com/privacy?hl=en-US

- ### Sentry.io

  Sentry collects Software errors, page loads, and API calls in order to to help us identify and fix bugs and improve performance:
  For more: https://sentry.io/privacy/

- ### YouTube

  If you choose to base your material creation in a video, you will be finding that video on YouTube. We cannot vouch for the quality or accuracy of every video on YouTube, so choosing an appropriate video is the responsibility of the user.

If this looks like more third-party services than others list, that is because we provide a broader list due to our commitment to transparency! Please make sure to verify ALL third party service providers used by all of the applications your school or district uses.

If we change our third party providers, we will update this policy and send an email to all our users to indicate the change.

Links to Third-Party Sites

When we give you a link to a website outside of our services (such as a Youtube video), it doesn't mean we endorse that website or what's on it. When you click on the link, you'll leave our site and go to another one. During this change, another company might collect your personal information. Remember, our Privacy Policy doesn't cover these other websites or any

information they gather after you leave our site. We suggest you carefully read the privacy policies of any website you visit.

Student Data

We do **not** collect any student data.

Age of Consent

Our Website is not intended for use by those under the age of 18, nor is it targeted to those under the age of 18. If you use our Services, you hereby represent and warrant that you are at least 18 years of age. No one under the age of 18 may provide any information to or on our Website. We do not knowingly collect Personal Data from those under the age of 18, nor do we knowingly sell or otherwise disclose the Personal Data of those under the age of 18.

If we become aware that we have collected Personal Data from persons under the age of 18 without verification of parental consent, we take steps to remove that information from our servers.

Right to Opt-In

By default, you will receive only necessary email communications from us, such as, for example, being informed of a change to this privacy policy.

You have the right to opt **IN** to receive promotional emails from us.

We will **NOT** share or sell your personal information with any third party intending to promote to you or share or target your email for promotional purposes.

Do Not Sell/Share/Target

Commitment to Privacy

We want to be clear: **We never sell or share your personal information.** This commitment is a core part of our privacy practices, regardless of the legal requirements to provide an opt-out.

Understanding Your Rights Under U.S. Privacy Laws

Some U.S. Privacy Laws require businesses to inform consumers of their rights to opt out of certain data processing activities, such as the sale or sharing of personal information for

targeted advertising. We are providing this information solely to comply with these laws, even though these activities are not part of our business practices.

- ### No Sale of Personal Information

  We do not sell your personal information to third parties, and you will never need to opt out of such practices with us because we simply don't engage in them.

- ### No Sharing for Targeted Advertising

  We do not share your personal information with third parties for targeted advertising. You are already opted out because we do not conduct these activities.

Opting Out of Cookie Tracking:

While we do not use cookies to sell or share your personal information, we understand you might want to manage your cookie preferences:

- You can adjust your cookie settings directly in each browser and device you use.
- If you have concerns or wish to discuss your privacy rights further, please contact us at security@questionwell.ai.

Other Cookies Options

Third parties may use cookies and other tracking technologies to recognize your device and/or to collect and record information about your visits to websites, including ours. These cookies and tracking technologies may be used to maintain or enhance website experience or functionality, measure the effectiveness of ads, track page usage, track paths taken while visiting websites, and provide advertisements to you based on our interests. These third parties may provide this data to us in an aggregated and anonymized way to help us understand our users' usage patterns as a whole and how we can improve the product and communication about the product. Again, we do not show ads or sell/share your data.

Supplemental Incident Response Plan

For a detailed overview of our Breach Incident Response Plan, please read the full plan, which covers:

- **Rapid Detection and Assessment:** How we quickly identify and evaluate the extent of a security breach.
- **Containment and Mitigation:** How we limit the breach's spread and impact while protecting sensitive data.

- **Eradication and Recovery:** How we remove the threat and restore affected services to full functionality.
- **Notification and Communication:** How we ensure timely and transparent communication with affected stakeholders.
- **Post-Incident Analysis:** How we learn from the incident to prevent future breaches

Supplemental European Union GDPR Statement

GDPR is the newest body of regulation regarding the handling of personal data for citizens of the European Union (EU). The primary objective of the GDPR is to give citizens control of their personal data. Our Services are compliant with the EU General Data Protection Regulation.

GDPR includes 11 chapters and nearly 100 articles. Below are some of the most relevant

articles.

- Article 5: “Principles relating to processing of personal data”: QuestionWell is a trusted steward of personal data. Data received from customers are to be used solely for purposes of providing educational services. Such data will not be sold or used for marketing purposes.
- Article 17: “Right to be forgotten”: Schools can choose to delete users from QuestionWell at any time. Individual users can choose to delete any data they’ve added to QuestionWell at any time. QuestionWell promptly deletes data associated with schools no longer working with QuestionWell.
- Article 32: “Security of processing”: QuestionWell keeps all personal data confidential and secure. QuestionWell team members are bound by contractual non-disclosure agreements. QuestionWell’s data security protections include: internal data management policies and procedures, limitations on access to personal data, data encryption (for both data in transit and at rest), data systems monitoring, incident response plans, and safeguards to ensure personal data is not accessed by unauthorized persons when transmitted over communication networks.
- Article 33: “Notification of a personal data breach to the supervisory authority”: GDPR requires notice to the supervisory authority within 72 hours of awareness of a personal data breach. Discovery of a security breach that results in an unauthorized release of personal data: QuestionWell shall promptly notify affected customers of such breach, shall conduct an investigation, and shall restore the integrity of its data systems as soon as possible. QuestionWell will fully cooperate and assist with required notices to those individuals affected by such breach.

- Article 35: “Data protection impact assessment”: QuestionWell conducts various security assessments of our systems. Certain security tests are conducted annually, others more frequently and some other tests are running constantly.
- Article 37: “Designation of a data protection officer”: QuestionWell maintains a designated data protection officer who is authorized to engage security reviews and impact product development.
- Article 44: “General principle for transfers”: To promote data sovereignty/data residency in GDPR, the regulation authorizes the European Commission to decide if a third country or territory, where data may be transferred, meets adequate levels of protection. As GDPR is new, no third country or territory has yet been approved by the Commission. QuestionWell customers are always in control over the storage and transmission of their personal data. Customers located in the EU or UK utilize a secure data center located within the EU zone (Frankfurt, Germany). No servers, outside of these options, are used to store data for EU or UK based customers.

Supplemental California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) gives consumers rights over the personal information that businesses collect about them. If you are a California resident, you have:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale or sharing of their personal information; and
- The right to non-discrimination for exercising their CCPA rights.
- The right to correct inaccurate personal information that a business has about them; and
- The right to limit the use and disclosure of sensitive personal information collected about them.

Although we are not required to (because we do not 1) have a gross annual revenue of over $25 million 2) buy, sell, or share the personal information of 100,000 or more California residents or households or 3) derive 50% or more of our annual revenue from selling California residents’ personal information) we follow the requirements of of this landmark legislation because we are committed to the security of our users.

How we use your information

Categories of Personal Information Collected	How it is collected	How it is used	Possible Disclosures for Business Purposes
Contact information (e.g., name, email address)	Google or Microsoft sign-in	• Provide our services • Communicate with you • Personalize our services • Improve the services (including debugging) • Provide security & prevent fraud • Comply with applicable laws	• Service providers (e.g. Stripe to verify your subscription) • Law enforcement if lawfully requested • With your consent
Device and online identifier information (e.g., IP address, browser type, operating system, general location inferred from IP address, and similar information)	You, through your device	• Provide, analyze and improve the services • Provide customer service • Protect security, prevent fraud, and for de-bugging • Comply with the law	• Service providers (e.g. Google Analytics to aggregate and analyze data) • Law enforcement in the event of a lawful request • With your consent
Service usage information (e.g., when and how your use the services)	You, through your device	• Provide, analyze and improve the services • Provide customer service • Protect security, prevent fraud, and for de-bugging • Comply with the law	• Service providers • Law enforcement in the event of a lawful request • With your consent
Financial and transactional information (e.g., payment account information)	You or Payment processors	• Process service fees • Communicate with you • Comply with legal requirements	• Payment processor service providers • Law enforcement in the event of a lawful request • With your consent

Non-Discrimination

We will not discriminate against you in a manner prohibited by the CCPA because you exercise your CCPA rights.

Supplemental GDPR Privacy Statement

Under EU Regulation 2016/679, also known as GDPR, QuestionWell is required to provide detailed information on our data processing practices to individuals in the European Economic Area. If you access our Services from within the EEA, this specific GDPR Privacy Statement applies to you.

Under the GDPR, QuestionWell at 30 Lake St #3, Somerville, MA, USA, is responsible for managing your personal information.

Legal Basis of Processing

QuestionWell processes your personal data based on Article 6(1)(b) of the EU GDPR, which permits processing necessary for the performance of a contract or to fulfill your requests.

Personal Data Transfers outside of the EEA

QuestionWell may transfer your personal data outside the EEA, potentially to countries like the U.S. with different data protection laws. We ensure an adequate level of protection by using measures approved by the European Commission, such as adherence to the Commission's adequacy decisions and the Standard Contractual Clauses (2010/87/EC or 2004/915/EC). We also implement strong physical, technical, and organizational security measures to protect your data against unauthorized access and other risks. All further data transfers are also subject to strict legal standards.

Data Retention

We keep your personal data only as long as necessary to deliver the services you've signed up for and to comply with the law. If you want us to delete it, you have the right to do so, by emailing us at security@questionwell.ai. It will be deleted within 60 days.

Your Rights

You can ask to see, change, or delete your personal data, or limit how we use it. You also have the right to transfer your data and to stop us from using your data for marketing. You can exercise these rights by managing your account settings or contacting us at security@questionwell.ai.

If you've given us consent, you can withdraw this consent at any time. This won't affect past data use. You also have the right to file a complaint with the relevant authority.

Profiling

QuestionWell does not use automated decision-making or profiling in a way that significantly impacts you legally or personally.

Sensitive Data

We do not collect biometric or specific location data. We only collect address and payment information if you pay for services, and this is securely processed by a third-party. We do not use this information for any other purpose.