

Privacy Policy

Effective Date: 17 April 2026

Last Updated: 16 April 2026

Studioware LLC (“Company,” “we,” “us,” or “our”) operates the website www.e-ballroom.com (e-Ballroom Dance Studio Management) (the “Website”) and the companion mobile applications e-Ballroom Kiosk, e-Ballroom, e-Ballroom Studio, and e-Ballroom Dancer (the “Apps,” and collectively with the Website, the “Services”).

We are committed to protecting your privacy. This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you use our Services. By accessing or using the Services, you agree to the terms of this Privacy Policy. If you do not agree, please do not use the Services.

This Policy applies to both the Website and the Apps unless otherwise noted. We may update this Policy from time to time; the updated version will be posted here with a revised “Last Updated” date. We will notify you of material changes via email, in-app notice, or on the Website. Your continued use after changes constitutes acceptance.

1. Information We Collect

We collect information in the following categories:

A. Information You Provide

- Account information: name, email address, username, password, phone number, company name (if applicable), and billing/shipping address.
- Profile and content data: any information or files you upload, post, or share while using the Services (e.g., documents, messages, expenses, transactions).
- Payment information: processed through third-party processors (we do not store full credit card numbers).
- Communications: messages you send to us via support, feedback forms, or email.
- Mobile-app-specific: push notification preferences, in-app preferences.

B. Information Collected Automatically

- Usage and analytics data: IP address, browser type, device type/model, operating system, app version, pages viewed, time spent, clickstream data, and referral source.
- Device identifiers: unique device ID, advertising ID, or other mobile identifiers (for Apps only).
- Cookies, pixels, and similar technologies: see Section 7 below.
- Location information: approximate location derived from IP address, or information as provided in a form
- Log data: error reports, crash logs, and diagnostic data.

C. Information from Third Parties

- Analytics providers (e.g., Azure Application Insights), advertising partners, or business partners.
- Payment processors or identity verification services.

2. How We Use Your Information

We use the collected information to:

- Provide, maintain, and improve the Services (including authentication, personalization, and feature functionality).
- Process transactions and send receipts or invoices.
- Communicate with you (service updates, support, marketing with your consent).
- Analyze usage trends and personalize your experience.
- Detect, prevent, and respond to security incidents, fraud, or abuse.
- Comply with legal obligations, enforce our Terms of Service, or protect our rights.
- For mobile apps: enable push notifications, offline functionality, or device-specific features (with your consent where required).

3. How We Share Your Information

We do not sell your personal information. We may share it in these circumstances:

- With service providers: cloud hosting (e.g., Azure), analytics (e.g., Google Analytics), customer support tools, payment processors, and email service providers — all under contracts that require them to protect your data.

- For legal reasons: in response to subpoenas, court orders, or to comply with laws (including CCPA/CPRA).
- Business transfers: in connection with a merger, acquisition, or sale of assets.
- With your consent: or at your direction (e.g., sharing workspace data with collaborators).
- Aggregated/de-identified data: we may share anonymized usage statistics publicly or with partners.

For mobile apps, certain third-party SDKs (e.g., Firebase, analytics libraries) may collect limited device data; these are disclosed in the App Store/Google Play privacy labels.

4. Data Security

We implement reasonable administrative, technical, and physical safeguards to protect your information (e.g., encryption in transit and at rest, access controls, regular security audits). However, no system is completely secure, and we cannot guarantee absolute security.

5. Data Retention

We retain personal information only as long as necessary for the purposes described or as required by law. Account data is typically retained while your account is active; we may retain de-identified or aggregated data indefinitely.

6. Your Rights and Choices

Depending on your location, you may have rights under laws such as the California Consumer Privacy Act (CCPA/CPRA), General Data Protection Regulation (GDPR), or similar laws:

- Access, correct, or delete your personal information.
- Opt out of certain processing (e.g., marketing, sale of data — though we do not sell data).
- Limit use of sensitive personal information (if applicable).
- Data portability.
- Object to or restrict processing.
- Withdraw consent (where processing is based on consent).

To exercise these rights, contact us at the details below. We will respond within the time required by law (usually 30–45 days). California residents may also submit a verifiable consumer request. We do not discriminate against users who exercise their rights.

7. Cookies, Tracking Technologies, and Do Not Track

We and our service providers use cookies, web beacons, and similar technologies on the Website and (where technically feasible) in the Apps to recognize your device, remember preferences, and analyze usage.

You can manage cookies through your browser settings. Most mobile devices allow you to limit tracking via device settings (e.g., “Limit Ad Tracking” on iOS or “Opt Out of Interest-Based Ads” on Android).

We currently do not respond to “Do Not Track” signals from browsers, but we honor global privacy controls where required.

8. Children’s Privacy

Our Services are not directed to children under 13 (or 16 in certain jurisdictions). We do not knowingly collect personal information from children. If we become aware that we have collected such data, we will delete it promptly. Parents/guardians may contact us if they believe their child has provided information.

9. International Data Transfers

If you are located outside the United States (our primary base of operations), your information will be transferred to and processed in the United States of America.

10. Third-Party Links and Services

The Services may contain links to third-party websites or services. We are not responsible for their privacy practices. We encourage you to review their policies.

11. Changes to This Privacy Policy

We may update this Policy to reflect changes in our practices or applicable laws. The new Policy will be effective upon posting. We will provide reasonable notice for material changes.

12. Contact Us

If you have questions or requests regarding this Privacy Policy or your data, please contact us:

Email: [support\[@\]e-ballroom\[.\]com](mailto:support[@]e-ballroom[.]com)

Mailing Address: [9500 Balcones Drive, Suite 100, Austin, TX 78731](#)

For data subject requests, please include sufficient information to verify your identity.

This is a sample template for informational purposes only and is not legal advice.

Privacy laws evolve, and requirements differ by jurisdiction and business model. We strongly recommend having a qualified attorney review and customize this document to ensure full compliance with applicable laws (including CCPA/CPRA, and app-store requirements). You should also maintain a separate Terms of Service and, for mobile apps, complete the privacy nutrition labels in the App Store and Google Play.

If you provide more details about your company name, service description, target audience, specific features, or jurisdictions served, I can refine this template further to better match your needs. Let me know how you'd like to proceed!