

STARTPLAYING PRIVACY POLICY

Last Updated: July 20, 2026

Welcome to Qualleta, Inc. d/b/a StartPlaying (“**StartPlaying**”, “**we**”, “**our**”, or “**us**”). We protect your privacy with the same intent and integrity we bring to our platform and services. This Privacy Policy outlines how we handle your personal data, whether you are a user, game master, applicant, or partner.

When you use our Services, including our websites (such as startplaying.games), platform, events, or other interactions, we collect only what is necessary to deliver the experience or respond to your requests.

Your privacy is not a tradeable asset. We do not sell personal data or profit from your sensitive information.

Our priority is providing a platform for immersive storytelling, not data monetization. Still, essential operations such as troubleshooting, processing transactions, and improving the platform require limited data from you and our service partners.

We collect data in line with industry standards and secure it using both technical and physical safeguards, including locked server rooms.

I. OUR DATA PROTECTION ROLES

We may act as both a Data Controller and, in limited cases, a Data Processor, depending on how personal data is collected and used through our Services.

A. DATA CONTROLLER

In most cases, StartPlaying acts as a Data Controller. We determine the purposes and means of processing personal data collected through our websites, platform, marketing activities, support channels, and community engagement.

As a Data Controller, we are responsible for safeguarding your data, defining how it is used, and enabling you to exercise your rights under applicable data protection laws.

B. DATA PROCESSOR

In limited cases, we may act as a Data Processor on behalf of third parties, meaning we process personal data solely under their instructions and not for our own purposes. In such instances, we are not responsible for determining the purpose or means of processing.

II. ELIGIBILITY

Our Services are intended for individuals who have reached the age 18 years old or older. We do not knowingly collect personal data from individuals under this age threshold. If you are under the age of 18, you may not use our Services without the verifiable consent of a parent or legal guardian.

Parents and guardians are responsible for ensuring that any individual under the age of 18 is under their supervision uses our Services in compliance with this Privacy Policy. Where required by law, we may implement age-gating or obtain active parental consent before allowing access to specific features.

If we learn that we have collected personal data from an individual under the applicable age threshold without proper consent, we will take immediate steps to delete the data in accordance with applicable law. This process is documented and completed within thirty (30) days, unless a shorter period is required.

If you believe we may have collected personal data from an individual under the age of 18 without verifiable consent, please contact us at support@startplayinggames.com.

III. HOW WE COLLECT DATA

We collect personal data through three main methods: data you provide directly, data provided by third parties, and data collected automatically.

A. DATA PROVIDED FROM YOU

We collect data you directly provide to us through:

Player Communication & Community Participation

- Website Visits. Information from interactions on our sites, such as messages, social media engagement, and Discord participation. Please be aware that content shared on public forums or social media channels may be visible to others and subject to the respective platform's privacy policies.
- Contacting Us. Personal details like your name, email address, and message content when you reach out to us. We ask that you do not include sensitive personal information unless necessary for resolution.
- Social Media Visits. Data from interactions with our profiles on platforms such as Twitter, Instagram, YouTube, and TikTok. This includes information such as IP address, browser type, device type, and operating system.
- Joining Discord. When you join our Discord server, your account information (e.g., username, user ID, participation) may be visible to us and to others within the server. In cases of community threats, harassment, or policy violations, we may retain limited records of communications for moderation and enforcement purposes.

Platform & Account Data

- Platform Data. Device data (e.g., type, operating system), user account information (e.g., session information and usage statistics).
- Job Applications. Applicant details, including name, contact information, employment and education history, and materials submitted during the hiring process (e.g., resume, CV).
- Partnerships. Professional contact information shared with us for business, promotional, or charitable purposes (e.g., name, title, company name, and collaboration details).

Diagnostics & Crash Reports

- Crash Reports. If a technical error or crash occurs, you may be prompted to submit a diagnostic report. These reports may include device data, system logs, crash traces, and file paths. Some file paths may contain indirect identifiers such as usernames. Submission is optional and used solely for troubleshooting. Logs are reviewed only by authorized personnel and retained temporarily for diagnostic purposes.

B. DATA PROVIDED FROM THIRD PARTIES

We also collect data from third-party sources to enhance and manage our Services:

- **Social Media and Video Conferencing Platforms**. Public profile information (e.g., username, profile picture, location) and interactions with our content (e.g., likes, comments, shares), subject to your platform settings.
- **Streaming Platforms**. Data such as usernames, avatars, follower counts, and interactions (e.g., comments, chat activity) during streaming events.
- **Analytics Providers**. Aggregated user interaction data used to understand community engagement and improve our Services.

C. DATA COLLECTED AUTOMATICALLY

We collect certain types of data automatically when you visit our websites or interact with our Services. This includes:

Device and Usage Data. We collect data about your device and usage, such as your IP address, device type, operating system, browser type, plugins, and general usage patterns. We do not determine your precise location from this data, and IP addresses are used only for approximate geographic reference (e.g., language settings, time zones, and server routing).

Log Data. We may collect log data automatically during your use of the Services, such as system events, session activity, and feature interactions. This data may include or be linked to personal information (e.g., device identifiers, IP addresses, or user IDs) when necessary to maintain system performance, detect bugs, and support ongoing product improvements. It is distinct from crash reports or diagnostics, which are user-submitted and described separately in this Policy.

Cookies. We use cookies and similar technologies (e.g., pixel tags, local storage) to enhance functionality, security, and performance. These may include:

- **Essential Cookies:** Enable basic website functionality, such as login sessions and security features. These cookies are mandatory.
- **Performance Cookies:** Analyze website usage and performance, helping us improve user experience.
- **Functional Cookies:** Remember user preferences and settings (e.g., language, theme) to enhance and personalize your browsing experience.

You can manage your cookie settings through your browser or device settings. Disabling certain cookies may impair certain functions of the Service.

Device and Digital Fingerprint. We may collect information about your online activities over time and across third-party sites or other online services. This may include device and digital fingerprint data, which is information derived from your device and browser configuration (such as device type, operating system, browser type and version, screen resolution, installed fonts or plugins, time zone, language settings, and IP address) that, alone or combined, may be used to identify or recognize your device or browser across sessions and services, even where cookies are disabled, blocked, or deleted.

We do not sell or share this data with third parties for advertising, analytics, or personalization purposes. This data is processed only by service providers acting on our behalf and is used exclusively to support detecting fraud and account misuse, functionality, security, and performance of our Services.

IV. DATA WE PROCESS

A. LEGAL BASIS FOR PROCESSING

StartPlaying processes personal data with a commitment to transparency, purpose limitation, and data minimization. We do not use personal data for behavioral profiling, predictive modeling, or automated decision-making. We also do not participate in Real-Time Bidding (RTB) or rely on the IAB Transparency and Consent Framework (TCF) for consent management.

We comply with applicable data protection regulations, including the California Consumer Privacy Act (“CCPA”), the General Data Protection Regulation (“GDPR”), and other global frameworks. We also monitor evolving global privacy laws, including new regulations in Canada, Brazil, and the United States to keep our practices current.

We process personal data under the following legal bases:

- **Consent.** We request your consent before placing non-essential cookies, sending marketing emails, or enabling third-party advertising.

- **Contractual Necessity.** We process data when it is required to fulfill our contract with you, for example, enabling gameplay, processing purchases through gaming platforms, or managing contests and giveaways.
- **Legitimate Interests.** We use your data to maintain our Services, enhance user experience, prevent fraud, analyze engagement, evaluate job applicants, and improve our offerings, provided such interests are not overridden by your privacy rights.
- **Legal Obligations.** We process personal data when necessary to comply with legal and regulatory obligations, such as tax, employment, and accounting requirements.
- **Vital and Public Interests.** In rare cases, we may process personal data to protect your vital interests or the public interest, for example, responding to emergencies.

In jurisdictions where legitimate interest is limited or requires opt-in consent (such as certain EU Member States), we rely on your explicit consent or contractual necessity instead. We maintain documentation of our processing activities to ensure our handling remains proportionate, lawful, and aligned with user expectations.

If you have any questions about how we determine our legal basis for a particular type of data, contact us at support@startplayinggames.com.

B. DATA MANAGEMENT OVERVIEW

We use different types of data to operate and improve our Services, support users, personalize communications, and meet our legal and business obligations. Examples include:

- Personal and contact information (e.g., name, email address, phone number)
- Account and profile information (e.g., username, preferences)
- Usage data (e.g., how you interact with our Services)
- Device and browser data (e.g., IP address, operating system)
- Biometric data (e.g., voice or facial recognition inputs, motion data), where applicable and collected with explicit consent (see Section V)

C. DATA PURPOSES

We process your data to:

- **Provide Services and Support.** Fulfill requests, maintain services, facilitate events or contests, deliver content, troubleshoot issues, and send necessary communications.
- **Personalize Communication.** Customize advertising, social integrations, content recommendations, and service notifications.
- **Support Legitimate Business Functions.** Operate, secure, and develop our Services; monitor and prevent fraud; comply with legal requirements; enforce policies; perform audits and analytics; and maintain operational integrity.

D. DATA DISCLOSURES

We may share or transfer your personal data to third parties where necessary to operate our Services, fulfill legal obligations, or protect our rights. When data is transferred internationally, we implement appropriate safeguards in accordance with applicable law, such as Standard Contractual Clauses (SCCs) for transfers from the European Economic Area or UK.

We may disclose your personal data under the following circumstances:

- With Your Consent. To third parties when you provide express consent.
- To Protect Rights or Comply with Law. As required by law, to protect safety or legal rights, or to support investigations.

- In Business Transfers. As part of a merger, acquisition, or similar event. We will obtain your consent as required by law.

E. CATEGORIES OF DATA RECIPIENTS

- Authorized Agents. With your verified authorization, we may share your data with designated agents making rights requests on your behalf.
- Partners. We may share limited usage or engagement data with our partners for operational purposes, such as coordinating launch events, community events, or analytics reporting. This data does not include purchase information, player identifiers, or personal communications.
- Service Providers (Processors). We share personal data with service providers who act solely on our behalf and under our instructions. These providers support infrastructure hosting, crash diagnostics, platform analytics, customer support, and operational tooling. All such providers are contractually prohibited from using personal data for their own purposes and are required to maintain appropriate safeguards.
- Community Platforms. Where applicable, we may receive or retain user messages or moderation data from community platforms such as Discord or Bluesky when necessary to investigate policy violations or ensure the safety of members in our community. Such records are stored securely and retained only for the duration necessary to fulfill its purpose.
- Law Enforcement and Courts. We may disclose data where required by law, court order, or to protect the safety, rights, or property of StartPlaying, our employees, our users, or the public. This includes cooperation with law enforcement or in response to lawful legal process.

V. BIOMETRIC DATA

Where our Services include features that involve biometric functionality — such as voice recognition, facial recognition, motion tracking, or similar technologies — we may collect biometric identifiers or biometric information as defined under applicable law, including the Illinois Biometric Information Privacy Act ("**BIPA**"), the Texas Capture or Use of Biometric Identifier Act ("**CUBI**"), and equivalent state or international frameworks.

We collect biometric data only where necessary to enable specific features, and only with your explicit prior consent. We do not sell, lease, trade, or profit from biometric data. Biometric data is retained only for the duration necessary to fulfill the purpose for which it was collected and is destroyed in accordance with applicable law — generally within three (3) years or upon termination of your use of the relevant feature, whichever occurs first.

Biometric data is subject to the same technical and organizational safeguards described in Section VI of this Policy. Where required by law, we maintain a publicly available written policy governing our retention and destruction schedule for biometric identifiers and information.

If you have questions about our biometric data practices or wish to withdraw consent, please contact us at support@startplayinggames.com.

VI. DATA STORAGE, RETENTION & SECURITY

A. STORAGE & INTERNATIONAL TRANSFERS

We store and process personal data using technical, physical, and administrative safeguards to meet global privacy and data transfer requirements. Your data may be collected in the United States and stored in the United States or other countries where StartPlaying or its service providers operate. By using our Services, you consent to such transfers, even where local laws may not provide equivalent protections.

Where applicable, we implement legal mechanisms to protect international data transfers, including Standard Contractual Clauses ("**SCCs**"), adequacy decisions under GDPR, and binding corporate rules or similar safeguards in other jurisdictions.

B. RETENTION & DELETION

We retain personal data only as long as necessary to deliver our Services, fulfill legal and regulatory obligations, resolve disputes, and enforce our policies. Where appropriate, we may aggregate, de-identify, or anonymize personal data and use it in accordance with applicable law and retain that non-personal information for analytical or archival purposes.

We store billing information and platform-specific user identifiers. StartPlaying does receive or retain your payment credentials or post-purchase identifiers.

Analytics data is collected and stored by service providers acting on our behalf. We do not maintain a proprietary analytics database.

If you contact us via our bug support email, that correspondence is stored in a separate inbox dedicated to technical troubleshooting. Individual messages may be deleted upon request, in accordance with applicable law.

Crash diagnostics and performance logs submitted by users are retained only for the time necessary to investigate and resolve the issue. Where supported, these logs are automatically deleted after a short retention window, typically not exceeding 90 days. Diagnostic data is processed solely for troubleshooting purposes and is not used for profiling, marketing, or behavioral analytics.

Data deletion requests will be honored in accordance with applicable law. If deletion is not immediately possible due to technical or legal constraints, the data will be securely stored and access restricted until deletion can be performed.

C. SECURITY MEASURES

We implement technical and organizational safeguards to protect your personal data, including encryption, access controls, security logging, and physical protections. We also require service providers to maintain equivalent standards under written agreements. While no system is completely secure, we actively monitor for vulnerabilities and seek to prevent unauthorized access, loss, misuse, or alteration of personal data.

D. USER RESPONSIBILITY & BREACH NOTIFICATION

You are responsible for protecting your own device access and login credentials. If you believe your account has been compromised, contact us immediately at support@startplayinggames.com.

If we become aware of a data breach affecting your personal data, we will notify you in accordance with applicable law and take appropriate steps to contain and remediate the incident.

Please note that our Services may link to third-party websites or tools not controlled by StartPlaying. We are not responsible for their privacy or security practices and encourage you to review those providers' policies separately.

VII. YOUR RIGHTS

We respect your privacy rights and are committed to providing you with meaningful choices and control over how your personal data is used. These rights may vary depending on your location, and we extend them to the fullest extent permitted by applicable law, including GDPR (EU/UK), CCPA (California), LGPD (Brazil), and other global frameworks.

You can exercise your rights by contacting us at support@startplayinggames.com. We may need to verify your identity before responding and will only request information already collected and internally verifiable.

Your Privacy Rights Include:

- **Right to Be Informed.** You have the right to know what personal data we collect, how we use it, and with whom we share it. We provide this information throughout this Policy and during key points of data collection.
- **Right of Access.** You can request access to the personal data we hold about you.
- **Right to Rectification.** You may request corrections to incomplete or inaccurate data. Where applicable, self-service tools may also be available for you to update your information directly.
- **Right to Erasure (Right to Be Forgotten).** You may request deletion of your personal data when it is no longer necessary, or when processing is based on your consent and you withdraw that consent.
- **Right to Restrict Processing.** You may request limited processing of your data in certain circumstances, such as when disputing accuracy or objecting to processing.
- **Right to Object.** You can object to processing based on legitimate interests or for direct marketing purposes.
- **Right to Data Portability.** You have the right to receive your data in a structured, commonly used, machine-readable format and transfer it to another controller.
- **Right Not to Be Subject to Automated Decision-Making.** You may object to decisions made solely based on automated processing, including profiling, where such decisions have legal or significant effects. We currently do not engage in such activities.
- **Use of Authorized Agents.** You may designate an authorized agent to make a verifiable rights request on your behalf under applicable laws. To do so, we may require written authorization and may also verify your identity directly before fulfilling the request.

If you have any questions or would like to exercise any of your individual rights, please contact us at support@startplayinggames.com.

VIII. YOUR CONTROLS

We understand the importance of privacy and strive to create an environment that respects your personal information. We are dedicated to our mission and committed to transparency. The following outlines the choices available to you and how to exercise them, enabling you to take an active role in managing your own data.

A. WITH US

StartPlaying Accounts. If you sign up for our Services and create an account, we provide you with options to customize your privacy preferences within your StartPlaying account settings. By adjusting these settings, you can actively manage the level of access and visibility of your personal information, ensuring that your privacy aligns with your individual preferences.

Privacy Settings. You can manage your privacy settings within our Services and customize your preferences to actively manage the level of access and visibility of your personal data. These controls enable you to adjust your social connections, visibility on leaderboards, and update your profile information. If prompted to submit a crash or diagnostic report, you may choose whether to share system-level information. These submissions are optional and not required to continue using the Services.

Communications. If you receive an unwanted email from us, you can use the unsubscribe link found at the bottom of the email to opt out of receiving future emails. Note that you will continue to receive transaction-related emails regarding products or Services you have requested. We may also send you non-promotional communications regarding us and our Services regarding our Services or updates to our Terms or this Privacy Policy.

Do Not Track. Do Not Track (“DNT”) is a privacy preference that users can set in certain web browsers. Please note that we do not respond to or honor DNT signals or similar mechanisms transmitted by web browsers.

Advertising. If you prefer not to receive marketing messages or sponsored content, please contact us at support@startplayinggames.com and we will ensure your preferences are updated accordingly.

Do Not Sell or Share My Personal Information (CCPA). If you are a resident of California, you have the right under the California Consumer Privacy Act (CCPA) to opt out of the sale or sharing of your personal information. To exercise this right, please contact us at support@startplayinggames.com with your request.

B. WITH THIRD-PARTIES

Our Services integrate with various third-party providers, including Community Platforms, Marketing Providers, and Security and Performance Providers. You can customize your privacy settings within your account settings through these providers to control the data that is shared with us. Where applicable, data is processed solely on StartPlaying's behalf under written agreements consistent with applicable law.

C. COOKIE CONTROLS

You may stop or restrict the placement of cookies on your device or remove them by adjusting your preferences as your browser or device permits. However, if you adjust your preferences, our Services may not work properly. Please note that cookie-based opt-outs may not apply to mobile applications. However, you can manage advertising preferences within mobile app settings or through your device's privacy controls. For example, Android and iOS offer options to limit ad tracking.

You can also opt-out of targeted advertising from data and advertising partners participating in self-regulatory programs through the websites provided by the online advertising industry.

If you have any questions or concerns regarding your privacy choices or how we handle your personal data, please do not hesitate to contact us at support@startplayinggames.com. You can also contact the support teams for each platform if you require further assistance managing your privacy settings.

IX. GENERAL PROVISIONS

A. POLICY UPDATES

We reserve the right to update this Privacy Policy at any time to reflect changes to our practices, legal requirements, or services. When we do, we will revise the "Last Updated" date at the top. Material changes will be posted prominently or communicated directly when required by law. Continued use of our Services after any update constitutes acknowledgement of the revised Privacy Policy.

B. CONTACT US

If you have questions about this Policy, please contact our Compliance Team at support@startplayinggames.com.

C. CONTACT A DATA PROTECTION AUTHORITY

If you have a concern about how we may collect and use data, please contact us. You also have the right to contact your local Data Protection Authority ("**DPA**") if you prefer. Where appropriate, your local DPA may also forward the matter to the Department of Commerce or FTC for consideration.

Last Updated: July 20, 2026